GEBHARDT Automation GmbH

GA DUPLEX/7-S

GA DUPLEX SMART-S

Sicherheitssysteme

Sicherheitshandbuch

Titel	GA DUPLEX-S Sicherheitshandbuch
Datei	GA DUPLEX-S Sicherheitshandbuch Rev00.00 280607.doc
Dokumenten-nummer	G0.HA.0003.028.00.088.00.00.I.D.E

Historieverzeichnis

Revisionsindex	Beschreibung	**E**rsteller **R**eviewpartner **F**reigebender	Datum
00.00	Dokument erstellt. Geltungsbereich-Info auf Seite 7 fehlt noch, deshalb Doku-Art Intern/Entwurf	E = SS R = MK F = UG	28.06.2007

Beteiligte von GEBHARDT Automation GmbH: Ulrich Gebhardt (UG), Wolfgang Paulicks (WP), Markus König (MK), Stephan Schild (SS), Dr. Peter Dellwig (PD)

Inhalt

1 ALLGEMEINE ANGABEN 6

1.1 KONTAKTINFORMATIONEN 6
1.2 GELTUNGSBEREICH UND STANDARDS 7
1.3 ALLGEMEINE HINWEISE 8
1.4 DOKUMENTENÜBERSICHT 9

2 SICHERHEITS-LEBENSZYKLUS 10

3 PRODUKTBESCHREIBUNG 12

3.1 GESAMTSYSTEM 12
3.2 PRINZIPIELLE ARBEITSWEISE 13
3.3 HARDWARE-KOMPONENTEN 14
3.4 FEHLERAUFDECKUNG 14
3.5 FEHLERREAKTION 15
FUNKTION UND BEDEUTUNG VON BEDIEN- UND ANZEIGEELEMENTEN 16
3.5.1 Elemente der MCxxx-S Karten 16
3.5.2 Elemente der ICU Karte 17
3.5.3 Elemente der FPR Karte 17
3.5.4 Elemente der DSPVCU Karte 18
3.5.5 Elemente des Lüfters 19
3.5.6 Elemente des DFAB-1oo2D 19
3.6 SICHERHEITSRELEVANTE ZEITEN 20
3.6.1 Systemreaktionszeit 20
3.6.2 Diagnose-Testintervall 20
3.6.3 Prozess-Sicherheitszeit 21
3.6.4 Wiederholungsprüfung 21

4 ENGINEERING DES PES-SYSTEMS 22

4.1 HARDWARE ENGINEERING 22
4.1.1 Spezifikation der Sicherheitsanforderungen 22
4.1.2 Hardware-Entwurf und Validierungsplanung 22
4.1.3 Systemintegration 22
4.1.4 Hardware-Engineering Checkliste 23
4.2 SOFTWARE ENGINEERING 23
4.2.1 Spezifikation der Sicherheitsanforderungen 23
4.2.2 Software-Entwurf und Validierungsplanung 23
4.2.3 SIL3-geprüfte Funktionsblöcke 24
4.2.4 Integration der PES Hardware und Software 24
4.2.5 Validierung der Software 24
4.2.6 Software-Engineering, Checklisten 25

5 MONTAGE UND INSTALLATION 26

5.1 PERSONELLE QUALIFIKATIONEN 26
5.2 SICHERHEITSTECHNISCHE RANDBEDINGUNGEN/ EINSCHRÄNKUNGEN 26
5.3 BEFESTIGUNGSHINWEISE UND ANSCHLUSSBELEGUNG 26
5.4 MONTAGE UND INSTALLATION, CHECKLISTE 27

6 FORCEN VON E/A-SIGNALEN 28

6.1 VORGEHENSWEISE 28
6.2 FORCEN VON E/A-SIGNALEN, CHECKLISTE 28

7 INBETRIEBNAHME 29

7.1 PERSONELLE QUALIFIKATIONEN 29
7.2 VORGEHENSWEISE 29
7.3 SOFTWARE-PROGRAMMÄNDERUNGEN 30
7.3.1 Programmänderungen und Erweiterungen 30
7.3.2 Parametrierung ändern 30
7.3.3 Online-Änderung 30

7.4 INBETRIEBNAHME, CHECKLISTEN ... 31

8 WARTUNG ... 32

8.1 PERSONELLE QUALIFIKATIONEN ... 32
8.2 VORGEHENSWEISE ... 32
8.3 KOMPONENTEN-AUSTAUSCH ... 33
8.4 WARTUNG, CHECKLISTE ... 33

9 ZUGANGSBERECHTIGUNG ... 34

9.1 BENUTZERANMELDUNG ... 34
9.2 SCHLÜSSELSCHALTER ... 34

10 DIAGNOSE UND FEHLERBEHEBUNG ... 36

10.1 VERFÜGBARKEIT VON DIAGNOSEDATEN ... 36
10.2 VERFÜGBARKEIT VON PROZESSDATEN ... 36
10.3 FEHLERNACHRICHTEN UND DEREN AUSWERTUNG ... 37

11 ALLGEMEINE TECHNISCHE DATEN ... 38

12 SICHERHEITSTECHNISCHE ANGABEN ... 39

12.1 BERECHNUNGSGRUNDLAGE ... 39
12.2 BEISPIELRECHNUNG ... 40

13 INDEX ... 42

Abbildungsverzeichnis

Abbildung 1: Dokumenten-Übersicht 9
Abbildung 2: Sicherheitslebenszyklus 10
Abbildung 3: Hardware-Sicherheitslebenszyklus 11
Abbildung 4: Software-Sicherheitslebenszyklus 11
Abbildung 5: Beispiele für Systeme und Vernetzung 12
Abbildung 6: Funktionsweise des GA DUPLEX-S Systems 13
Abbildung 7: Frontblende und Elemente der MCxxx-S Karten 16
Abbildung 8: Frontblende und Elemente der ICU Karte 17
Abbildung 9: Frontblende und Elemente der FPR Karte 18
Abbildung 10: Frontblende und Elemente der DSPVCU Karte 18
Abbildung 11: Frontblende und Elemente des Lüfters 19
Abbildung 12: DFAB-1oo2D Feldanschlussmodul 19
Abbildung 13: Benutzeranmeldung 34
Abbildung 14: Schlüsselschalter Running/Maintenance 34
Abbildung 15: Zuverlässigkeits-Blockdiagramm für 1-aus-2D 40

Tabellenverzeichnis

Tabelle 1: Checkliste Hardware-Engineering 23
Tabelle 2: Checkliste Software-Engineering, Systemintegration 25
Tabelle 3: Checkliste Software-Engineering, Programmierung 25
Tabelle 4: Checkliste Software-Engineering, Validierung 25
Tabelle 5: Checkliste Montage und Installation 27
Tabelle 6: Checkliste Forcen von Signalen 28
Tabelle 7: Checkliste Inbetriebnahme 31
Tabelle 8: Checkliste Inbetriebnahme, Programmänderung 31
Tabelle 9: Checkliste Wartung, Kartenaustausch 33
Tabelle 10: 15% PES-Ausfallwahrscheinlichkeiten und SIL-Einstufung 41
Tabelle 11: Sicherheitsintegrität der Hardware, Typ B-Teilsysteme 41

1 Allgemeine Angaben

1.1 Kontaktinformationen

GEBHARDT Automation GmbH

Oelkinghauser Str. 12 a
D- 58256 Ennepetal
Deutschland

Tel.: +49 (0)2333 7908 - 0
Anrufe werden an Wochentagen (Mo ... Fr) zwischen $8^{\underline{00}}$ und $17^{\underline{00}}$ Mitteleuropäischer Zeit (MEZ / CET, GMT+1) beantwortet.
FAX: +49 (0)2333 7908 - 24

Web: www.gebhardt-automation.de

Support support@gebhardt-automation.de
Informationen info@gebhardt-automation.de

1.2 Geltungsbereich und Standards

Dieses Dokument beschreibt die folgenden Systeme:

- GA DUPLEX/7-S
- GA DUPLEX SMART-S

jeweils ab Hardware-Revision 00, Datum .

Die sicherheitsgerichteten Regelungs- und Schutzsysteme der GEBHARDT Automation GmbH sind vom TÜV entsprechend IEC 61508 für SIL 3 zertifiziert sowie konform zur CE:

TÜV Rheinland Group
TÜV Industrie Service GmbH
Automation, Software und Informationstechnologie
Am Grauen Stein
D - 51105 Köln

Zertifikat und Prüfbericht Nr.
Programmierbare elektronische Sicherheitssysteme
GA DUPLEX/7-S und GA DUPLEX SMART-S

GEBHARDT Automation GmbH ist berechtigt das oben gezeigte Prüfzeichen für die „**F**unktionale **S**icherheit“ im Zusammenhang mit den SIL3 zertifizierten Systemen zu verwenden.

Die Systeme sind entsprechend der folgenden Standards und Normen entwickelt und wurden bezüglich der wesentlichen relevanten Sicherheitsanforderungen geprüft:

- **IEC 61508 Part 1 – 7: 1998 + 1999**
  Functional safety of programmable electronic systems
- **DIN EN 954-1: 03.97**
  Sicherheit von Maschinen; Sicherheitsbezogene Teile von Steuerungen
  Teil 1: Allgemeine Gestaltungsleitsätze
- **EN ISO 13849-1: 2006**
  Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen -
  Teil 1: Allgemeine Gestaltungsleitsätze
- **DIN EN 60204 Teil 1: 11.98**
  Sicherheit von Maschinen - Elektrische Ausrüstung von Maschinen
  Teil 1: Allgemeine Anforderungen
- **DIN EN 50178: 1998**
  Ausrüstung von Starkstromanlagen mit elektronischen Betriebsmitteln
- **IEC 61131-2: 2003**
  Programmable controllers
  Part 2: Equipment requirements and tests

1.3 Allgemeine Hinweise

Alle technischen Angaben und Hinweise in diesem Handbuch wurden mit größter Sorgfalt erarbeitet und kontrolliert. Trotzdem sind Fehler nicht ganz auszuschließen. GEBHARDT Automation GmbH weist darauf hin, dass weder eine Garantie noch eine juristische Verantwortung oder irgend eine Haftung für Folgen die auf fehlerhafte Angaben zurückgehen übernommen werden kann.

Für gefahrlose Installation, Inbetriebnahme, Betrieb und Instandhaltung der GA DUPLEX-S Sicherheitssysteme ist die technisch einwandfreie Umsetzung der in diesem Handbuch enthaltenen Sicherheitshinweise durch qualifiziertes Personal Voraussetzung.

Nicht qualifizierte Eingriffe in die Systeme, wie z.B. Nichtbeachten von Sicherheitshinweisen dieses Handbuchs, können die Ausführung von Sicherheitsfunktionen beeinträchtigen und evtl. zu schweren Sach-, Umwelt- oder Personenschäden führen, für die GEBHARDT Automation GmbH keine Haftung übernehmen kann.

Die GA DUPLEX-S Systeme werden unter Beachtung der einschlägigen Sicherheitsnormen entwickelt, gefertigt und geprüft. Sie dürfen nur für die in den Beschreibungen vorgesehenen Einsatzfälle mit den spezifizierten Umgebungsbedingungen und nur in Verbindung mit zugelassenen Fremdgeräten verwendet werden.
Änderungen an den Systemen sind verboten. Für Reparatur und Wartung sind nur die speziell für diese Systeme zugelassenen Ersatzteile erlaubt.

Die Software der GA DUPLEX-S Systeme darf nicht kopiert werden, außer als Sicherheitskopie.
Sie sind nicht berechtigt, die Software zurückzuentwickeln (reverse engineering), zu dekompilieren oder zu disassemblieren.

Die in diesem Handbuch genannten Produkte der GEBHARDT Automation GmbH sind teilweise als Warenzeichen geschützt.
Dies gilt gegebenenfalls auch für andere genannte Hersteller und deren Produkte.

Die vollständige oder auszugsweise Wiedergabe dieses Dokuments ist ohne schriftliche Erlaubnis von GEBHARDT Automation GmbH nicht gestattet.

Alle Rechte und technische Änderungen vorbehalten.

1.4 Dokumentenübersicht

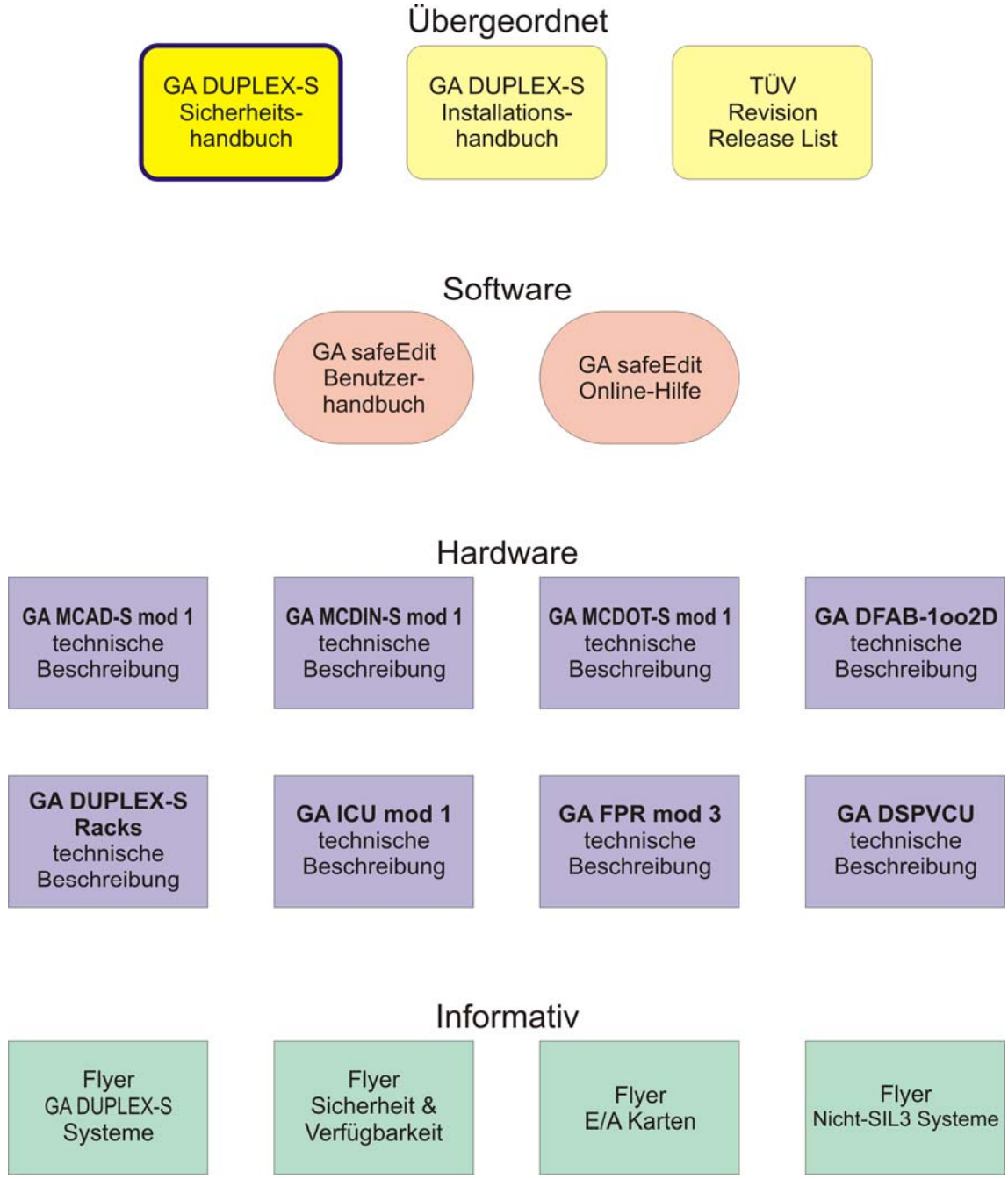

Abbildung 1: Dokumenten-Übersicht

Die Abbildung gibt einen Überblick über die relevanten Dokumente zu den GA DUPLEX-S Sicherheitssystemen. Im vorliegenden Sicherheitshandbuch wird bei Bedarf auf die entsprechenden Dokumente verwiesen.
Die informativen Dokumente geben nur eine Kurzübersicht über das jeweilige Thema und sind nicht sicherheitsrelevant. Auf sie wird im Sicherheitshandbuch kein Bezug genommen.

2 Sicherheits-Lebenszyklus

Zur systematischen Herangehensweise an Planung, Auslegung und Analyse der Sicherheit betrachtet die IEC 61508 den gesamten Lebenszyklus des Systems: angefangen von der Planung, über den Vertrieb, über Wartung und Reparatur, bis hin zur Ausserbetriebnahme. Der Lebenszyklus ist in 16 Phasen unterteilt und definiert für jede Phase notwendige Tätigkeiten und Maßnahmen zur Erreichung der geforderten Sicherheitsintegrität.

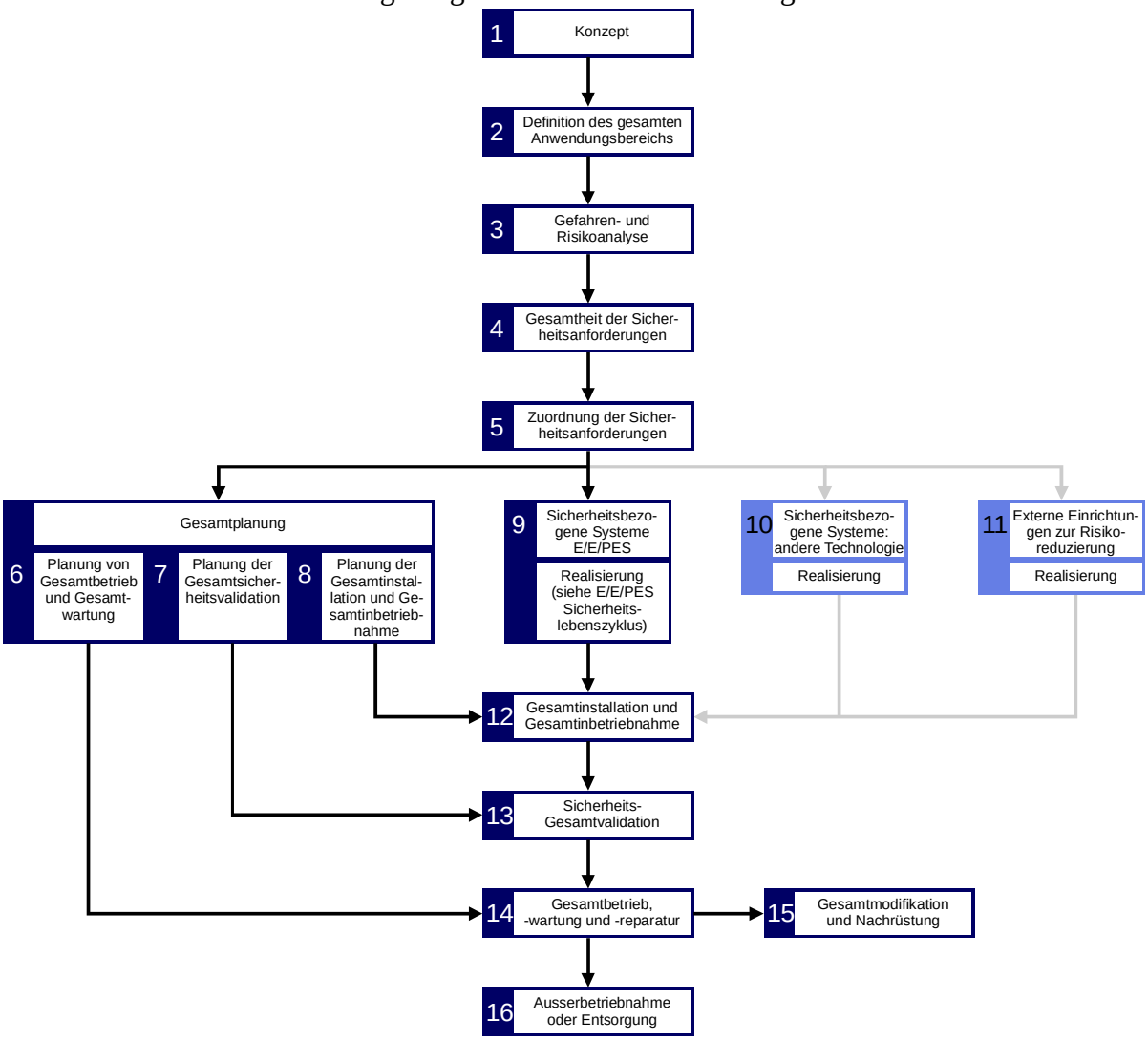

Abbildung 2: Sicherheitslebenszyklus

Dieses Dokument bezieht sich hauptsächlich auf Phase 9 des gesamten Sicherheitslebenszyklus, das PES-System. Zu dessen Realisierung gibt der entsprechende Teil-Lebenszyklus für PES Hardware und Software jeweils weitere Details an.
Die Phasen 10 (andere Technologien, z.B. mechanische Not-Aus Vorrichtungen) und 11 (externe Einrichtungen, z.B. Fluchtwege, Schutzwälle) sind im Umfang dieses Dokuments nicht relevant.

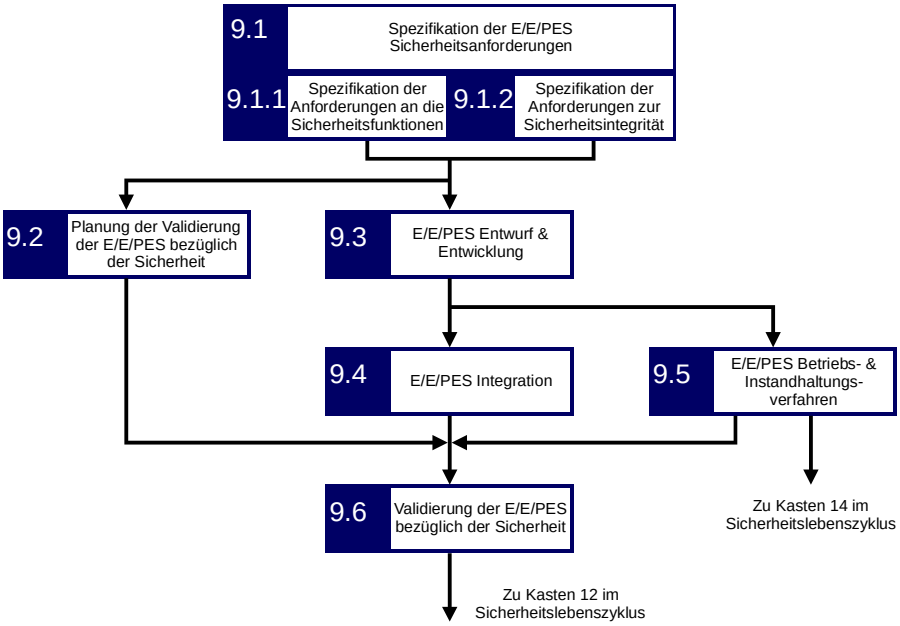

Abbildung 3: Hardware-Sicherheitslebenszyklus

Die Phasen des Hardwarelebenszyklus sind bei der Planung und Auslegung des PES-Systems zu berücksichtigen. Im Dokument werden zu jeder Phase Tätigkeiten und Maßnahmen definiert.

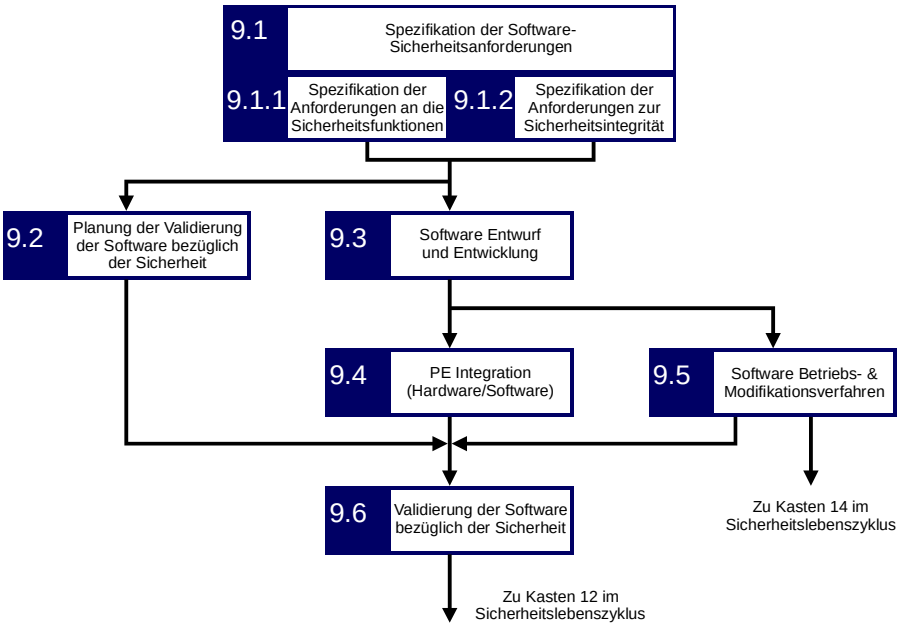

Abbildung 4: Software-Sicherheitslebenszyklus

Die Phasen des Softwarelebenszyklus sind bei der Planung und Auslegung der Software für das PES-Systems zu berücksichtigen. Im Dokument werden zu jeder Phase Tätigkeiten und Maßnahmen definiert.

3 Produktbeschreibung

3.1 Gesamtsystem

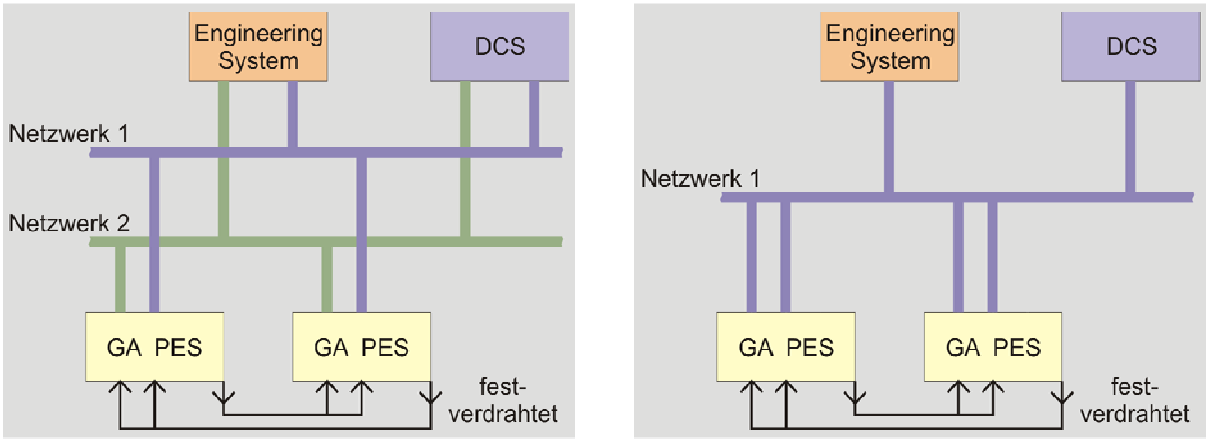

Abbildung 5: Beispiele für Systeme und Vernetzung

Ein GA DUPLEX-S System besteht im Regelfall aus mindestens einem PES-System, einem Engineering-System und einem Visualisierungssystem (Leitsystem, DCS). Dabei übernimmt das PES-System völlig selbstständig die eigentliche Sicherheitsfunktion. Im Normalbetrieb kann das PES-System von keinem anderen System (PES, Engineering oder DCS) beeinflusst werden. Nur im Wartungsmodus, der über den Hardware-Schlüsselschalter verriegelt ist, kann durch autorisierte Benutzer vom Engineering-System eine Einflussnahme auf das System erfolgen.
Sicherheitsgerichtete Kommunikation zwischen mehreren PES-Systemen ist z.Zt. nur über fest verdrahtete E/A-Signale möglich.

Das Engineering-System ist ein PC mit dem Betriebssystem Windows (2000 oder XP) und dem Programmierwerkzeug GA safeEdit. Dieses System kann nach Aktivierung des Wartungsmodus für Inbetriebnahme und Wartungsaufgaben am Sicherheitssystem benutzt werden. Im Normalbetrieb wird das Engineering-System nicht benötigt, es kann aber jederzeit für erweiterte Systemdiagnosen verwendet werden.
Optional kann für Engineeringaufgaben derselbe PC verwendet werden wie für die Visualisierung. Beides kann auf einem PC parallel betrieben werden.

Das Visualisierungssystem erhält über offene Kommunikationsschnittstellen Lesezugriff auf Daten und Informationen des PES-Systems. Es hat keinerlei Eingriffsmöglichkeit in die Steuerung. Neben der normalen Steuerungs-Visualisierung werden auch Diagnoseinformationen zur PES-Hardware angezeigt.

Abbildung 5 zeigt als Beispiel zwei Varianten für ein Gesamtsystem, bestehend aus Engineering-System, Leitsystem (DCS, Visualisierung) und zwei PES-Systemen:
Die linke Seite zeigt redundante Netzwerke. Dabei wird die Kommunikation für Engineering und Visualisierung zu jeder der redundant arbeitenden DUPLEX-Einzelkomponenten unabhängig durchgeführt. So ist selbst im Fall einer Netzwerkstörung immer noch die volle Kommunikation zu den nicht gestörten Komponenten vorhanden. Engineering- und DCS-System müssen dazu redundante Netzwerkkarten verwenden.

Die rechte Seite zeigt ein einfaches, nicht redundantes Netzwerk. Die redundanten PES-Komponenten verwenden zur Kommunikation alle dasselbe Netzwerk. Bei einer Netzwerkstörung ist die gesamte Kommunikation betroffen.
Die Netzwerkkommunikation läuft rückwirkungsfrei zu den eigentlichen Sicherheitsfunktionen des Systems.
Das Netzwerk nach Abbildung 5 kann um weitere Systeme aller Typen (PES, DCS, Engineering) erweitert werden. Im selben Netzwerk können auch normale, nicht sicherheitsgerichtete Steuerungssysteme verwendet werden.

3.2 Prinzipielle Arbeitsweise

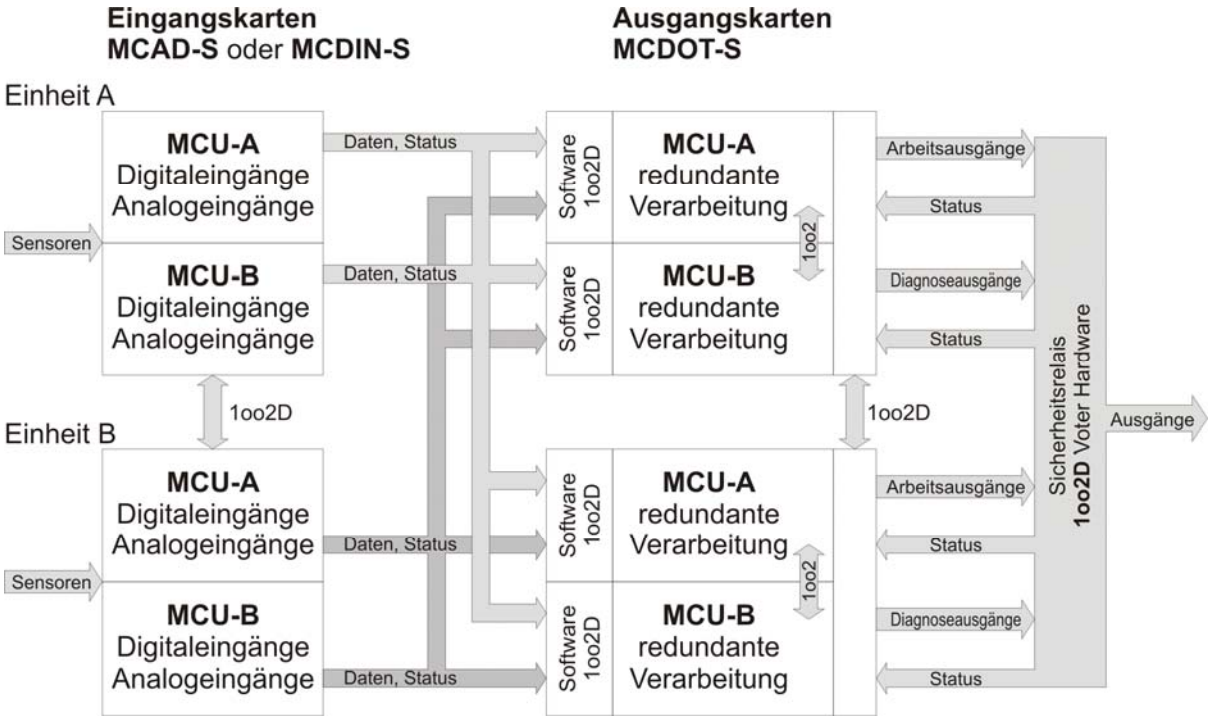

Abbildung 6: Funktionsweise des GA DUPLEX-S Systems

Die Abbildung zeigt die prinzipielle Arbeitsweise eines GA DUPLEX-S Systems. Eingangskarten (Typ MCDIN-S für Digitaleingänge, MCAD-S für Analogeingänge) lesen Feldsignale ein. Auf den Karten befinden sich jeweils zwei redundant arbeitende MCU-Prozessoren. Auf beiden Prozessoren, MCU-A und MCU-B sind alle Eingangssignale bekannt. Über den internen Datenbus, ICU-Kommunikationskarten und FPR-Speicherkarten werden die Daten an die Ausgangskarten weitergeleitet (Typ MCDOT-S für Digitalausgänge, Typ MCDA-S zukünftig für Analogausgänge). Auf diesen Karten werden Sicherheitsanwendungen (z.B. Emergency Shutdown Logik) programmiert. Der größte Teil der Sicherheitsanwendungen wird in der Regel verteilt auf den jeweiligen intelligenten Ausgangskarten ausgeführt. Zur Signal-Vorverarbeitung können auch Daten zwischen den jeweils zwei parallel arbeitenden Eingangskarten ausgetauscht werden. Z.B. kann eine Auswahl zwischen den Signalen der zwei Einheiten erfolgen: Min, Max oder Average.

Voting von Eingangsdaten

Zur Erhöhung der Verfügbarkeit und für den Online-Austausch von Eingangsmodulen wird empfohlen, das 1oo2D-Voting für Eingangsdaten in der Sicherheitsanwendung stets zu aktivieren. Wird ein Fehler des Eingangssignals oder Eingangskanals erkannt, so wird auf ein 1oo1D Voting degradiert.

Mittels Voting können auch Abweichungen der redundanten Feldsignale untereinander analysiert werden. Die zulässige Abweichung ist dabei in der Sicherheitsanwendung parametrierbar. Ist sie zu hoch, wird der Status des betroffenen Kanals auf „fault“ gesetzt. (siehe *GA safeEdit Benutzerhandbuch, AIN-Block*)

Voting von digitalen Ausgangsdaten

Die Ergebnisse der redundanten Verarbeitung von MCU-A und MCU-B auf den Ausgangskarten werden kartenintern per Software als 1-aus-2 Auswahl verknüpft. Diese Ergebnisse werden anschließend zwischen den Einheiten A und B ausgetauscht. Systemintern wird über diese ausgetauschten Signale ein 1-aus-2D Voting in Software durchgeführt bevor die Berechnungsergebnisse auf den DFAB-1oo2D Ausgangsvoter gelangen (siehe Kapitel 3.5.6). Am Ausgang des Voters steht das eigentliche Feldsignal zur Verfügung.
Die Zustände der Signalausgänge und der Relais des DFAB-1oo2D Ausgangsvoters werden als Statusinformationen analog zurückgelesen und erlauben die Fehlerdiagnose. Zum sicheren Abschalten kann die MCDOT-S Ausgangskarte zusätzlich im Fehlerfall über einen zweiten, getrennten Abschaltweg immer den sicheren Zustand herstellen.

3.3 Hardware-Komponenten

Für die Verwendung in den GA DUPLEX-S Systemen sind nur die in der Versionsliste der geprüften und zugelassen Komponenten aufgeführten Hardwarekomponenten zugelassen.
Siehe *Revision Release List.*

3.4 Fehleraufdeckung

Zur Erreichung eines möglichst hohen Fehleraufdeckungsgrades sind zahlreiche Selbsttests, so genannte BITs (build in tests), auf den Sicherheitskarten implementiert. Dazu gehören die einmalig nach dem Einschalten der Karten durchlaufenden Power-On Tests sowie zahlreiche zyklisch aufgerufenen BITs und die dynamischen BITs. Die zyklischen BITs werden in festen Zeitabständen wiederholend durchgeführt und die dynamischen sind abhängig von z.B. dem Empfangen von Datenpaketen anderer Teilnehmer im System. Die BITs testen den Microcontroller, die Erfassung von Feldsignalen, die internen und externen Speicher, die Sicherheitsanwendung und die Kommunikation zwischen den Modulen. (siehe *GA safeEdit Benutzerhandbuch, GA technische Beschreibung MCxxx-S*) .

Sicherheitsrelevante Einstellungsmöglichkeiten zur Fehleraufdeckung:

Aktivierung / Deaktivierung von Eingängen

Für ungenutzte Eingänge kann die Diagnose deaktiviert bzw. unterdrückt werden. Deaktivierte Eingänge werden in den FailSafe-Zustand („low“ für digitale Eingänge; 0.0 mA für analoge Eingänge) versetzt (siehe *GA technische Beschreibung MCxxx-S*). Die Messergebnisse der aktiven Eingänge werden auf Fehlerzustände hin geprüft, so dass ein kritischer Zustand im Feld schnell erkannt wird.

Testintervalle für feldseitige Selbsttests

Die Durchführung und Testintervalle von feldseitigen Selbsttests auf den Ein- und Ausgangskarten sind nach der Projektierung des Systems nur durch den Hersteller GEBHARDT Automation GmbH konfigurierbar. Diese Einstellungen sind passwortgeschützt (siehe technische Beschreibung der Sicherheitskarten). Ohne ausdrücklichen Kundenwunsch werden die Standardwerte eingestellt.

Diagnose der MCAD-S:
Die Schwellwerte für Fehlerzustände der analogen Strom- und Frequenzeingänge sind konfigurierbar. Bei jeder Prozesswertmessung wird die Über- bzw. Unterschreitung von sicherheitsrelevanten Schwellen geprüft. (siehe *GA technische Beschreibung MCAD-S*).

3.5 Fehlerreaktion

Während des Betriebs auftretende und erkannte Fehler werden frontseitig über 2x 4 LEDs signalisiert. In den entsprechenden technischen Beschreibungen zu den Karten wird die Bedeutung der Signalisierungs-LEDs erläutert.

Ein erkannter Fehler auf den Eingangskarten führt dazu, dass der Status der relevanten Daten auf „fault“ gesetzt wird. Erst nach erfolgter Reparatur und Quittierung wird der Status wieder auf „okay“ gesetzt. Das optional einstellbare Software-Voting der betroffenen Eingangsdaten degradiert von 1oo2D auf 1oo1D, solange bis der Fehler behoben ist.

Ein erkannter Fehler auf den Ausgangskarten führt ausgangsseitig unverzüglich zum Abschalten (de-energize to trip) der jeweiligen Einheit oder des jeweiligen Kanals. Es erfolgt somit eine Degradierung von 1oo2D auf 1oo1D. Der 1oo2D Voter erlaubt es, dass mit den Ausgängen der zweiten, noch intakten Einheit bis zur Reparatur des defekten Moduls weiter gearbeitet werden kann. Die Reparatur kann in der Regel während des Betriebs (unter Spannung) durch erfahrenes Personal innerhalb kurzer Zeit erfolgen (siehe auch MTTR, Seite 39). Sollte vor Ablauf einer eingestellten Zeit (siehe *technische Beschreibung MCDOT-S*) das defekte Modul nicht getauscht worden sein, erfolgt auch eine Abschaltung der noch intakten 1oo1D-Einheit, und somit wird der Feldkontakt geöffnet. Die tolerierbare maximale Länge der einstellbaren Ablaufzeit richtet sich nach den Anforderungen der realisierten Schutzfunktionen und insbesondere nach der geforderten SIL-Stufe des gesamten Systems.

Werden unterschiedliche Ergebnisse je Einheit berechnet, ohne dass eine Einheit einen Fehler erkannt hat, werden alle Ausgänge der beteiligten MCDOT-S Karten deaktiviert und die relevanten Feldkontakte geöffnet.

Funktion und Bedeutung von Bedien- und Anzeigeelementen

3.5.1 Elemente der MCxxx-S Karten

Alle E/A-Karten haben identische Bedien- und Anzeigeelemente in der Frontblende. Die Abbildung zeigt am Beispiel der MCDIN-S Karte die LEDs für Diagnoseanzeigen sowie den Auswurfhebel.

Abbildung 7: Frontblende und Elemente der MCxxx-S Karten

Es werden spezielle Führungsschienen im Baugruppenträger verwendet. Ein in den Schienen integrierter Klipp (der mit dem Gehäuse verbunden ist) schafft zusammen mit einem Führungsstift (am Hebel, Bild mitte-rechts) vor dem Einstecken der Karte eine galvanische Verbindung der Karten-Frontblende zum Baugruppenträger-Gehäuse. Dadurch können u.A. statische Aufladungen vor dem Stecken der Karte abgebaut werden.
Mit Hilfe eines Kipphebels mit integriertem Mikroschalter kann das Ziehen der Karten nach dem Lösen der Halsschrauben einfach durch Aushebeln nach unten erfolgen. Eine zum Hebelgriff passende Modulschiene (Bild unten-rechts) ermöglicht eine entsprechende Hebelfunktion. Vor dem Ziehen muss jedoch der integrierte Mikroschalter gedrückt werden (roter Knopf). Dadurch wird die Karte ausgeschaltet; ansonsten ist ein Ziehen der Karte durch eine mechanische Verriegelung nicht möglich. Damit wird ein unbeabsichtigtes Ziehen der Karte, bevor sie abgeschaltet ist, verhindert.
Durch die mechanische Kopplung von schwarzem Kipphebel und Mikroschalter wird kurz bevor die DSP-Bus Steckverbindung unterbrochen wird, die Karte ausgeschaltet. Die Beeinflussung der Signale auf dem Bus während des Ziehens wird auf einen unkritischen Wert minimiert.
Mit Hilfe des Kipphebels kann die Karte auch wieder eingehebelt werden. Beim Einstecken wird die Karte erst wieder eingeschaltet nachdem die Bus-Steckverbinder eine „saubere“ Verbindung zum DSP-Bus aufweisen. Undefinierte Zustände beim Einstecken und damit verbundene Signalverfälschungen werden dadurch vermieden bzw. minimiert.

Je vier frontseitige gelbe LEDs für MCU-A und MCU-B geben Auskunft über den aktuellen Betriebszustand der beiden redundanten Microcontroller.

Für weitere Informationen siehe technische Beschreibungen der entsprechenden Karte oder der DUPLEX-S Racks.

3.5.2 Elemente der ICU Karte

Die mechanische Verbindung der ICU-Karten im Baugruppenträger ist identisch mit den MCxxx-S Karten, siehe Abbildung und Beschreibung von Führungsschiene und Auswurfhebel.

Abbildung 8: Frontblende und Elemente der ICU Karte

Im unteren Bereich der Frontblende befinden sich LEDs zur Zustands- und Funktionsanzeige der ICU-Karte:

- Ethernet Link/Act: LED gelb zeigt physikalische Verbindung und Aktivität der Ethernet-Netzwerkschnittstelle an.
  Normaler Zustand der LED ist gelb blinkend.
- Ethernet 100: LED grün zeigt schnelle Ethernet-Verbindung mit 100 MBit an, LED aus zeigt langsame 10 MBit Verbindung.
  Normaler Zustand der LED ist grün.
- T/R1 und T/R2: LED gelb zeigt Aktivität an seriellen Schnittstellen COM1 bzw. COM2 an, Transmit/Receive 1 und 2.
  COM1 ist eine reine Programmierschnittstelle, die LED im Betrieb immer aus.
  COM2 kann für serielle Modbus RTU Kommunikation benutzt sein, LED aus oder blinkend.
- ARC: LED gelb zeigt Aktivität der Arcnet-Netzwerkverbindung an. Für DUPLEX-S Systeme wird Arcnet nicht verwendet, Normalzustand ist LED aus.
- MA: LED grün zeigt richtige Funktion der ICU-Karte an. Im normalen Betriebszustand ist die Karte als Master aktiv, LED grün.
- R/U: im DUPLEX-S System keine Bedeutung, Zustand ist egal.
- WDG: LED rot zeigt Watchdogfehler der ICU-Karte an. Im Normalbetrieb muss die LED aus sein.

3.5.3 Elemente der FPR Karte

Die mechanische Verbindung der FPR-Karten im Baugruppenträger ist identisch mit den MCxxx-S Karten, siehe Abbildung und Beschreibung von Führungsschiene und Auswurfhebel.

Abbildung 9: Frontblende und Elemente der FPR Karte

Von den vier auf der FPR-Karte (Four Ported RAM) zur Verfügung stehenden Speicherbereichen wird von den zwei Einheiten A, und B im DUPLEX-S System nur jeweils ein Bereich genutzt. Die Bereiche C und D werden nicht verwendet.

Die grünen LEDs zeigen Schreibzugriffe (WR, write) an, wenn eine Einheit Daten in ihren FPR-Bereich schreibt. Jede Einheit kann nur auf ihren eigenen Bereich A oder B schreiben. Normaler Zustand ist ein schnelles Flackern der grünen LEDs.
Die gelben LEDs zeigen Lesezugriffe auf den jeweiligen Speicherbereich an. Jede Einheit kann Daten aus allen Bereichen lesen. Normaler Zustand ist ein schnelles Flackern der gelben LEDs.

3.5.4 Elemente der DSPVCU Karte

Abbildung 10: Frontblende und Elemente der DSPVCU Karte

Die zwei DSPVCU Spannungsüberwachungskarten kontrollieren die Sekundärspannungen jeweils eines der beiden redundanten Netzteile. Sie erzeugen bei Über- oder Unterspannung

ein externes Fehlersignal. Die Karte hat einen einfachen Auswurfhebel, ohne mechanische Verriegelung, Potentialausgleich und elektrische Abschaltung. Die Karte ist nicht mit dem Datenbus des Systems verbunden.

Die frontseitigen roten LEDs zeigen Fehler in der Spannungsüberwachung der einzelnen Betriebsspannungen des GA DUPLEX-S Systems an, „Lower Limit“ für Unterschreitung, „Upper Limit“ für Überschreitung der Spannung. Im Normalbetrieb müssen alle roten LEDs aus sein.

Die grüne LED „Power Good“ ist die Sammelmeldung wenn alle Spannungen korrekt sind. Im Normalbetrieb muss diese LED grün leuchten.

3.5.5 Elemente des Lüfters

Abbildung 11: Frontblende und Elemente des Lüfters

Die LEDs an der Frontblende des Lüfters zeigen dessen Betriebszustand an. Im Normalbetrieb muss die grüne „on“ LED leuchten, die rote „alarm“ LED darf nicht leuchten.

Eine Störung des Lüfters, z.B. durch mechanische Blockierung, setzt die rote „alarm“ LED auf an. Nach Behebung der Störung muss durch Drücken des „reset“ Knopfes der Alarm quittiert werden, bevor die rote LED ausgeht.

Nach Lösen der links (nicht gezeigt) und rechts (im Bild sichtbar) befindlichen Halteschrauben kann der Lüfter im laufenden Betrieb nach vorne aus dem System herausgezogen und gewechselt werden.

Eine Störung des Lüfters hat keine direkte Auswirkung auf den Zustand des Systems. Sie kann allerdings zu einer Überhitzung des Gesamtsystems oder von Einzelkomponenten führen.

3.5.6 Elemente des DFAB-1oo2D

Abbildung 12: DFAB-1oo2D Feldanschlussmodul

Das Feldanschlussmodul DFAB-1oo2D benutzt keine direkten Anzeigeelemente. Im Bereich links oben sieht man zwei Sicherungsautomaten. Die Betätigungsstifte dieser Automaten müssen im eingedrückten Zustand sein.

An den Relais kann man den An/Aus-Zustand der einzelnen Digitalausgänge der redundanten Einheiten A und B erkennen. Es wird unterschieden zwischen Arbeits-Relais („worker“) und Diagnose-Relais („diagnostic“). Die Diagnose-Relais folgen im Normalfall ihren gegenüber liegenden Arbeits-Relais. Sie dienen im Fehlerfall dazu, die betroffene Einheit zu entkoppeln. Im Normalfall haben die zusammengehörigen Relais beider Einheiten jeweils die identische Position. Während des Selbsttests des DFAB Moduls (Walking Change) wird kurzfristig immer die testende Einheit entkoppelt während ein Relais auf die entgegengesetzte Position gesetzt wird.
Auf diesem externen DFAB ist mit Hilfe von zwangsgeführten Sicherheitsrelais, die nach dem Ruhestromprinzip arbeiten, eine 1-aus-2D Mehrheitsauswahl (mit Diagnose) realisiert.

Weitere Details siehe *GA DFAB-1oo2D technische Beschreibung*.

3.6 Sicherheitsrelevante Zeiten

3.6.1 Systemreaktionszeit

Die Systemreaktionszeit ist die Zeit zwischen Auftreten einer externen Anforderung und der Antwort des PES-Systems. Sie enthält die Zeiten zwischen Auftreten und Erkennen der Anforderung, interner Verarbeitung mit Setzen des Hardwareausgangs und Reaktionszeit der Relais am DFAB Ausgangs-Voter.
Die Zeit für die interne Verarbeitung der Signale, die Programmzykluszeit, ist abhängig von der Komplexität der gesamten Steuerungsfunktionen, die auf einer MCDOT-S Ausgangskarte verarbeitet werden. Für Details zur Programmzykluszeit siehe das *GA safeEdit Benutzerhandbuch*.
Im Normalfall ist die maximale Systemreaktionszeit die zweifache Programmzykluszeit plus 15 ms als Antwortzeit der DFAB-Relais.

Ausnahmen von normaler Systemreaktionszeit können auftreten bei:

- Verteilung einer Sicherheitsfunktion auf mehrere MCDOT-S Karten
- hardwired Kommunikation zwischen verschiedenen Systemen

3.6.2 Diagnose-Testintervall

Im PES-System werden neben den eigentlichen Sicherheitsfunktionen ständig Diagnosefunktionen ausgeführt um fehlerhaftes Verhalten aufzudecken. Das Diagnose-Testintervall ist der Zeitraum, in dem diese Tests durchgeführt und wiederholt werden.

Das Diagnose-Testintervall der Komponenten im PES-System muss so gewählt sein, dass die Wahrscheinlichkeit eines zufälligen Hardwareausfalls kleiner oder gleich dem in der Spezifikation der Sicherheitsanforderungen festgelegten Ausfallgrenzwert ist.
In einem nicht redundanten PES-System müsste dazu die Summe aus Diagnose-Testintervall und der im Fehlerfall folgenden Fehlerreaktion kleiner als die Prozess-Sicherheitszeit sein.

Im GA DUPLEX-S System ist die Wahrscheinlichkeit eines gefährlichen Hardwareausfalls (Ausfall einer Sicherheitsfunktion ohne Wechsel in den sicheren Zustand) aufgrund der Redundanz und des sicherheitsgerichteten Funktionskonzepts extrem gering, so dass obige For-

derung erfüllt ist. Das Diagnose-Testintervall ist parametrierbar. Nur ein autorisierter Mitarbeiter der GEBHARDT Automation GmbH darf die Einstellung des Testintervalls ändern. Eine Anpassung durch den Anwender ist nicht möglich.

3.6.3 Prozess-Sicherheitszeit

Die Prozess-Sicherheitszeit ist die Zeit vom Auftreten einer Prozessstörung bis zum Eintreten eines gefährlichen Zustands. Das Sicherheitssystem muss innerhalb dieser Zeit den Prozess in den sicheren Zustand gebracht haben. Dabei muss der gesamte Sicherheitskreis aus Sensor, PES-System und Aktor berücksichtigt werden.

Für das PES-System kann die Systemreaktionszeit als Berechnungsgrundlage zur Einhaltung der Prozess-Sicherheitszeit angenommen werden.

Das Diagnose-Testintervall geht normalerweise nicht direkt in die Berechnung ein.

3.6.4 Wiederholungsprüfung

Ziel der Wiederholungsprüfung (Proof Test) ist es, das PES-System nach einer bestimmten Einsatzzeit möglichst vollständig zu prüfen und damit wieder in den „Neu-“Zustand zu bringen. Dabei sollen besonders die mit den normalen Diagnosen nicht aufdeckbaren Ausfälle erkannt werden.
Als Minimum müssen alle vom PES-System ausgeführten Sicherheitsfunktionen gemäß der Spezifikation geprüft werden.

Die Wiederholungsprüfung soll in Intervallen von nicht mehr als 10 Jahren ausgeführt werden.
Durch Verkürzung der Proof Test Intervalle kann die Versagenswahrscheinlichkeit des Systems verringert werden. Standardmäßig werden 10 oder 3 Jahre angenommen.

4 Engineering des PES-Systems

Auslegung, Programmentwicklung und Realisierung des Sicherheitssystems erfolgen im Rahmen des Sicherheitslebenszyklus in Kasten 9, „Sicherheitsbezogene Systeme E/E/PES“, siehe *Abbildung 2: Sicherheitslebenszyklus* auf Seite 10.
Abbildung 3: Hardware-Sicherheitslebenszyklus und *Abbildung 4: Software-Sicherheitslebenszyklus* geben detaillierte Vorgaben zu verschiedenen Phasen des Engineerings sowie zu erforderlichen Maßnahmen und Tätigkeiten.

4.1 Hardware Engineering

4.1.1 Spezifikation der Sicherheitsanforderungen

Projektabhängig wird eine Liste aller Sicherheitsanforderungen erstellt. Darin werden alle Anforderungen an Sicherheitsfunktionen und Sicherheitsintegrität konkretisiert. Diese Liste dient als Grundlage für Hardware- und Softwareentwurf des PES-Systems.

4.1.2 Hardware-Entwurf und Validierungsplanung

Im Hardware-Entwurf wird die zur Erfüllung der Sicherheitsanforderungen erforderliche PES-Hardware geplant. Festgelegt wird die Anzahl und Art der PES-Systeme sowie die jeweils verwendeten E/A-Karten in diesen Systemen.
Parallel zum Hardwareentwurf erfolgt direkt die Validierungsplanung.

Dazu sind die folgenden Maßnahmen erforderlich:

- Zu jeder Sicherheitsfunktion wird der PES-interne Sicherheitskreis von Eingängen bis zu Ausgängen festgelegt. Alle Ausgangssignale eines Sicherheitskreises sollten sich auf einer MCDOT-S Karte befinden, nicht aufgeteilt auf mehrere Karten. Alle Eingangssignale müssen im selben DUPLEX-S System erfasst werden. Auf den Eingangskarten kann eine Signalvorverarbeitung stattfinden.
  Im Einzelfall können Signale festverdrahtet zwischen mehreren PES-Systemen ausgetauscht werden, dies ist aber nach Möglichkeit zu vermeiden. Diese Signale müssen in der Validierungsplanung berücksichtigt und gezielt auf ihre Systemreaktionszeit untersucht werden.
- Auf jeder MCDOT-S Karte dürfen mehrere Sicherheitskreise geplant werden. Normalerweise ist eine etwa gleichmäßige Aufteilung sinnvoll, um ähnliche Systemreaktionszeiten auf den einzelnen Karten zu erhalten.
- Wechselwirkungen durch gemeinsame Eingangssignale in verschiedenen Sicherheitsfunktionen müssen genau eingeplant und dokumentiert werden.
- Die Verteilung der E/A-Signale auf PES-Systeme und deren E/A-Karten muss dokumentiert und in die Validierungsplanung aufgenommen werden.
- Die Verteilung der Sicherheitsfunktionen auf PES-Systeme und MCDOT-S Ausgangskarten muss dokumentiert werden und geht in Validierungsplanung und Software-Engineering ein.

4.1.3 Systemintegration

Die Systemintegration plant die Integration der PES-Systeme in das gesamte Sicherheitskonzept.

Zu berücksichtigen sind die folgenden Punkte:

- Integration der Systeme im Schaltschrank, mit externer Hardware.

- Integration zwischen mehreren PES-Systemen, mit besonderer Berücksichtigung von festverdrahteter Kommunikation zwischen den Systemen.
- Integration der PES-Systeme in das Gesamtkonzept, bestehend aus Engineering-System und Visualisierungssystem (DCS).
- Netzwerkaufbau bezüglich Redundanz und Adresskonfiguration.

4.1.4 Hardware-Engineering Checkliste

Nr.	Beschreibung	Check
1	Anzahl E/A-Karten entsprechend Sicherheitsanforderungen, einschließlich Reservesignalen.	
2	Position der E/A-Karten im System entsprechend Vorgaben	
3	Analoge Frequenzeingänge mit passender Grenzfrequenz und Festlegung des Sondentyps.	
4	Sicherheitsfunktionen bezüglich der Ausgangssignale sinnvoll kartenweise geplant.	
5	Festverdrahtete Kommunikation zwischen PES-Systemen: Systemreaktionszeiten berücksichtigen.	
6	Anschlusskabel mit passenden Kabeltypen und –Längen	
7	Netzwerkaufbau: Entfernungen, Kabellängen und –verlegung, Kabeltypen (Kupfer, Glasfaser), Switches, Router, Redundanz, Adressierung	

Tabelle 1: Checkliste Hardware-Engineering

4.2 Software Engineering

4.2.1 Spezifikation der Sicherheitsanforderungen

Die Liste der Sicherheitsanforderungen nach Kapitel *Spezifikation der Sicherheitsanforderungen* auf Seite 22 wird erweitert um Informationen zu den E/A-Signalen. Zu jedem Digitalsignal wird der Öffner/Schließer (NO/NC) Zustand definiert, zu Analogsignalen der physikalische Wertebereich.
Für jede Sicherheitsfunktion wird die erforderliche Sicherheitszeit spezifiziert.
Für jede Sicherheitsfunktion wird die konkrete Funktionsweise spezifiziert.

4.2.2 Software-Entwurf und Validierungsplanung

Die im Hardware-Entwurf geplante Aufteilung der Sicherheitsfunktionen auf die PES-Hardware wird entsprechend der Software-Spezifikation in Sicherheitsapplikationen umgesetzt. Für jede Sicherheitsfunktion wird dabei der interne Sicherheitskreis von Eingangssignal über Applikation bis zum Ausgangssignal betrachtet.
Als Programmiersystem wird GA safeEdit verwendet. Informationen zur Handhabung gibt das Dokument *GA safeEdit Benutzerhandbuch*.
Bei der Umsetzung sind die folgenden Maßnahmen zu berücksichtigen:

- Programmierung der einzelnen Sicherheitskreise auf den in der Hardwareauslegung geplanten MCDOT-S Ausgangskarten.
- Fehlerverhalten bei Signalfehler für jedes Eingangssignal in jedem Sicherheitskreis definieren. 1oo2, Available/Error, ... Dokumentieren und in Validierungsplan aufnehmen.
- Betriebsartenumschaltungen in Sicherheitskreisen genau analysieren. Validierungsplan ***aller*** Modi unter besonderer Berücksichtigung des Umschaltzeitpunkts vorbereiten.

- Wechselwirkungen zwischen Sicherheitskreisen (ein Hardware-Eingang in mehreren Kreisen verwendet, Zwischenzustände an anderer Stelle verwendet) genau dokumentieren, in Validierungsplan aufnehmen.
- Intern zu berechnende Grenzwerte für Analogsignale festlegen, physikalisch und intern normiert, mit Hysterese. Dokumentieren und in Validierungsplan aufnehmen.
- Einschaltverhalten der Sicherheitskreise planen, mit Validierungsplan.
- Signalnachführung für Hardwareersatz (Spare-Karte) im DUPLEX-S System für Funktionsbausteine mit Speicherfunktion (RS-Flipflop) planen, mit Validierungsplan.

4.2.3 SIL3-geprüfte Funktionsblöcke

Die meisten von GA safeEdit zur Verfügung gestellten Funktionsblöcke sind für die Verwendung in SIL3-Sicherheitsfunktionen geprüft. Sie dürfen ohne Einschränkungen für die Applikationsprogrammierung verwendet werden. Das *GA safeEdit Benutzerhandbuch* enthält die aktuelle Liste der SIL3-geprüften Funktionsblöcke.
Die nicht in der Liste aufgeführten Funktionsblöcke sind für den Gebrauch in Sicherheitsfunktionen nicht zugelassen. Sie dürfen nur für nicht-sicherheitsrelevante Funktionen verwendet werden.

4.2.4 Integration der PES Hardware und Software

Im Rahmen der Hardware- und Softwareintegration werden PES-Hardware und -Software aufeinander abgestimmt. Zusätzlich wird die Integration ins Gesamtsystem, insbesondere bezüglich der Systemdiagnose im Visualisierungssystem, berücksichtigt.

Bei der Integration sind die folgenden Maßnahmen zu berücksichtigen:

- Hardware- und Softwarekonfiguration aufeinander abstimmen (Slotkonfiguration, Netzwerk, Zugriffe auf Eingangskarten, ...).
- Signaldiagnosen (Kabelbruch/Kurzschluss) für verwendete Signale aktivieren, für Reservesignale deaktivieren.
- Systemreaktionszeit der einzelnen Ausgangskarten MCDOT-S mit kompletter Software bestimmen und mit spezifizierten Sicherheitszeiten vergleichen. Reserve für IBN-Erweiterungen einplanen!
- Speicherplatzauslastung der einzelnen Ausgangskarten MCDOT-S mit kompletter Software bestimmen, Reserve für IBN-Erweiterungen einplanen!
- Relevante Diagnoseinformationen des PES-Systems sollten im Visualisierungssystem angezeigt werden, um auf Systemdegradation oder kritische Zustände hinzuweisen und ein rechtzeitiges Eingreifen zu ermöglichen.

4.2.5 Validierung der Software

Die Validierung der Software erfolgt mit dem Programmiersystem GA safeEdit und verwendet die folgenden Verfahren:

- Prüfung auf Syntax und Parametrierung, im Programmiersystem.
- Simulation, offline auf PC, ohne spezifische PES-Hardware.
- Online-Debug auf PES-Hardware, mit geforcten E/A-Signalen, ohne Feldsignale
- Online-Debug auf PES-Hardware, mit Feldsignalen von Testhardware (Schaltschrankbau).
- Im Rahmen der Inbetriebnahme erfolgt der Softwaretest anschließend mit echten Feldsignalen im Maschinenstillstand, dann an der laufenden Maschine.

4.2.6 Software-Engineering, Checklisten

Nr.	Beschreibung	Check
1	Hardware- und Software-Konfiguration stimmen überein	
2	Netzwerkkonfiguration in Hardware und Software korrekt	
3	Systemreaktionszeit jeder MCDOT-S Ausgangskarte passend zu den Sicherheitszeiten der entsprechenden Sicherheitsanforderungen. Reserve für Erweiterungen während der Inbetriebnahme ist ausreichend.	
4	Speicherplatz der MCDOT-S Karten ausreichend, auch für Softwareerweiterungen während der Inbetriebnahme.	
5	Signalfehlererkennung Kabelbruch/Kurzschluss für benutzte Signale aktiviert, für Reservesignale deaktiviert.	
6	Zugriff auf alle erforderlichen Diagnoseinformationen zum Visualisierungssystem (DCS) spezifiziert / programmiert.	
7	Systemkonfiguration projektabhängig entsprechend der Vorgaben (Timeouts, Zeiten, Kommunikationspfade, ...)	

Tabelle 2: Checkliste Software-Engineering, Systemintegration

Nr.	Beschreibung	Check
1	Signalzustand und Wertebereich für jedes Signal entsprechend Vorgaben.	
2	Signalfehler-Verhalten (1oo2) für jedes Eingangssignal in jeder Sicherheitsfunktion entsprechend Vorgabe parametriert.	
3	Analoge Grenzwerte entsprechend Vorgaben. Normierung und Hysterese.	
4	Wechselwirkungen zwischen Sicherheitsfunktionen entsprechend den Vorgaben.	
5	Einschaltverhalten der Sicherheitsfunktionen nach Vorgabe.	
6	Signalnachführung (Tracking) für Funktionsbausteine mit Speicherfunktion implementiert.	
7	Nur SIL3-geprüfte Funktionsblöcke für die Programmierung von Sicherheitsfunktionen verwendet.	

Tabelle 3: Checkliste Software-Engineering, Programmierung

Nr.	Beschreibung	Check
1	Syntax- und Parameterprüfung: keine Fehler oder Warnungen	
2	Simulation, offline auf PC: Verhalten nach Vorgaben	
3	Online-Debug auf PES-System, ohne Feldsignale, mit Forcen im Maintenance-Modus	
4	Online-Debug auf PES-System, mit Feldsignalen und Testhardware, im Running-Modus	

Tabelle 4: Checkliste Software-Engineering, Validierung

5 Montage und Installation

5.1 Personelle Qualifikationen

Montage und Installation der Hardware müssen ausschließlich durch qualifiziertes Personal erfolgen. Dieses Personal muss mit den Warnungen und Hinweisen der technischen Handbücher vertraut sein.
Qualifiziertes Personal im Sinne der technischen Hardwarebeschreibungen sind Personen, die mit Aufstellung, Montage, Inbetriebnahme und Betrieb dieser Hardware vertraut sind und über die ihren Tätigkeiten entsprechenden Qualifikationen verfügen, wie z.B.:

- Ausbildung und Unterweisung bzw. Berechtigung, Stromkreise und Baugruppen bzw. Systeme gemäß den aktuellen Standards der Sicherheitstechnik ein- und auszuschalten, zu erden und zu kennzeichnen.
- Einweisung in das projektspezifische Sicherheitskonzept.
- Erfahrung mit der Installation von GA DUPLEX-S Komponenten.
- Schulung in der E/A-Signaldiagnose mit dem Programm GA safeEdit kann erforderlich sein.
- Ausbildung und Unterweisung gemäß den aktuellen Standards der Sicherheitstechnik in Pflege und Gebrauch angemessener Sicherheitsausrüstungen.
- Schulung in Erster Hilfe.

5.2 Sicherheitstechnische Randbedingungen/ Einschränkungen

Die Systeme dürfen nur in normaler Umgebung eingesetzt werden. Säurehaltige Umgebungsluft muss vermieden werden, insbesondere dürfen keine H_2S Anteile enthalten sein.

5.3 Befestigungshinweise und Anschlussbelegung

Befestigung und elektrisches Anschließen ist entsprechend der technischen Beschreibung der jeweiligen Komponenten und des *Installationshandbuches* auszuführen.

Allgemein gelten die folgenden Punkte:

- Grundsätzlich ist auf mechanisch stabile Befestigung zu achten.
  Komponenten müssen spielfrei eingebaut sein und dürfen nicht wackeln oder vibrieren.
  Alle Schrauben müssen richtig festgezogen sein.
- Um eine ausreichende Kühlung zu gewährleisten müssen die Komponenten in der richtigen Einbaulage mit genügend Abstand zu anderen Geräten oder Abdeckungen platziert werden.
- Signalleitungen müssen getrennt von elektrischen Anschlussleitungen verlegt sein. Allgemein ist auf eine ordentliche Verlegung und Beschriftung von Kabeln zu achten.
  Signalleitungen müssen bei Bedarf gegen Überspannungen oder Überströme geschützt werden.
- Die Versorgungsspannungen müssen im erlaubten Bereich liegen.
- Die Komponenten müssen EMV-gerecht eingebaut werden. Dazu ist bei Baugruppenträgern auf richtige Erdung im Schaltschrank zu achten.
- Fast jede Baugruppe enthält elektrostatisch gefährdete Bauteile. Elektrostatische Entladungen durch den menschlichen Körper o.a. müssen daher unbedingt vermieden werden, z.B. durch vorheriges Berühren von geerdeten Metallteilen (metallisier-

te und geerdete Gehäuse ,Wasserleitung, Einbaurahmen, etc.). Das gilt insbesondere vor dem Wechsel einer Baugruppe.

5.4 Montage und Installation, Checkliste

Nr.	Beschreibung	Check
1	Optische Prüfung: keine Beschädigungen; Geräte sauber eingebaut; Kabel ordentlich verlegt; Beschriftungen von Komponenten vorhanden und richtig.	
2	Mechanische Prüfung: Schrauben angezogen; Geräte fest montiert, kein Schwingen oder Wackeln.	
3	Verkabelung: Stecker richtig aufgesteckt, evtl. verschraubt; Erdungsanschlüsse korrekt ausgeführt; Trennung von Signal- und Anschlussleitungen	
4	Elektrische Einschaltprüfung: alle LEDs zeigen Normalzustand	

Tabelle 5: Checkliste Montage und Installation

6 Forcen von E/A-Signalen

6.1 Vorgehensweise

Mittels Forcen können alle Eingangs- und Ausgangssignale des PES-Systems in den gewünschten Zustand gebracht werden. Da in diesem Fall die normalen Sicherheitsfunktionen nicht mehr ausgeführt werden können darf das Forcen nur unter genau geklärten Bedingungen zur Inbetriebnahme und zu Wartungszwecken eingesetzt werden. Die Vorgehensweise zum Forcen ist im *GA safeEdit Benutzerhandbuch* beschrieben.

Beim Forcen sind die folgenden Punkte zu beachten:

- Einflussanalyse: Vor dem Forcen muss genau geklärt und verstanden sein, welche Auswirkungen auf das PES-System und auf den Prozess möglich sind. Dabei sind auch eventuelle Vorraussetzungen im PES-System, Maschinen- oder Prozess-seitig, klar zu definieren.
- Das Forcen darf nur durch qualifiziertes Personal im Rahmen von Inbetriebnahme- oder Wartungsarbeiten durchgeführt werden.
  Im Normalbetrieb sind geforcte Signale nicht zulässig, da die betroffenen Sicherheitsanforderungen eingeschränkt oder nicht mehr erfüllt sind.
- Die Vorgehensweise zum Erreichen des gewünschten Zustands muss eindeutig verstanden sein. Welche Signale müssen in welcher Reihenfolge geforct werden? Die Redundanz im DUPLEX-S System ist zu berücksichtigen.
- Die Vorgehensweise zum Aufheben des Forcens muss eindeutig verstanden sein.
- Wenn durch das Forcen Schutzmassnahmen beeinträchtigt werden sind evtl. Sicherungsmaßnahmen (Gefahrenzonen absperren, usw.) erforderlich.
- Da normale Sicherheitsanforderungen eingeschränkt oder nicht mehr erfüllt werden müssen entsprechende Notfallmaßnahmen vorbereitet sein.

6.2 Forcen von E/A-Signalen, Checkliste

Nr.	Beschreibung	Check
1	Wurden die Auswirkungen auf das System und den Prozess analysiert und vollständig geklärt?	
2	Sind die System- und Prozessvoraussetzungen für das Forcen gegeben?	
3	Ist die Vorgehensweise zum Forcen des benötigten Zustands eindeutig geklärt?	
4	Ist die Vorgehensweise zum Aufheben des Forcens und zur Rückkehr in den Normalbetrieb eindeutig geklärt? Wie wird kontrolliert?	
5	Wurden evtl. notwendige Sicherungsmaßnahmen außerhalb des Systems durchgeführt?	
6	Sind ausreichende Notfallmaßnahmen außerhalb des Systems vorbereitet?	

Tabelle 6: Checkliste Forcen von Signalen

7 Inbetriebnahme

7.1 Personelle Qualifikationen

Inbetriebnahme der Hardware muss ausschließlich durch qualifiziertes Personal erfolgen. Dieses Personal muss mit den Warnungen und Hinweisen der technischen Handbücher vertraut sein.
Qualifiziertes Personal im Sinne der technischen Hardwarebeschreibungen sind Personen, die mit Aufstellung, Montage, Inbetriebnahme und Betrieb dieser Hardware vertraut sind und über die ihren Tätigkeiten entsprechenden Qualifikationen verfügen, wie z.B.:

- Ausbildung und Unterweisung bzw. Berechtigung, Stromkreise und Baugruppen bzw. Systeme gemäß den aktuellen Standards der Sicherheitstechnik ein- und auszuschalten, zu erden und zu kennzeichnen.
- Ausbildung und Unterweisung in der Verwendung der Software GA safeEdit für die Inbetriebnahme von SIL3 Sicherheitssystemen.
- Einweisung in das projektspezifische Sicherheitskonzept.
- Einweisung in die projektspezifische Applikationsprogrammierung.
- Detaillierte Kenntnisse der Installation der Sicherheitssysteme im Schaltschrank.
- Einweisung in die zu steuernden Maschinen/Anlagen und den Prozess.
- Ausbildung und Unterweisung gemäß den aktuellen Standards der Sicherheitstechnik in Pflege und Gebrauch angemessener Sicherheitsausrüstungen.
- Schulung in Erster Hilfe.

7.2 Vorgehensweise

Die Inbetriebnahme ist nur mit dem Programmiersystem GA safeEdit möglich. Es ist als Engineering-System zum Programmieren, Konfigurieren und für viele Diagnosefunktionen erforderlich. Parallel dazu ist eine Visualisierung am Leitsystem (DCS) möglich, die während der Inbetriebnahme ebenfalls getestet und bei Bedarf angepasst werden muss.

Während der Inbetriebnahme des PES-Systems wird hauptsächlich die Maintenance-Betriebsart benutzt. Der Inbetriebnehmer benötigt den oder die Schlüsselschalter sowie die erforderlichen Passwörter für die Freigabe des Maintenance-Modus.
Während Inbetriebnahmeunterbrechungen ist sicherzustellen, dass das System gegen unerlaubte Zugriffe geschützt ist.

Tätigkeiten während der Inbetriebnahme und dabei zu beachtende Punkte sind:

- Während der Inbetriebnahme werden die Sicherheitsfunktionen des PES-Systems noch nicht erfüllt. Daher sind entsprechende Sicherungs- und Notfallmaßnahmen vorzubereiten und zu treffen.
- Erstes Einschalten der PES-Hardware: Kontrolle auf ordnungsgemäßen elektrischen Anschluss aller Komponenten.
- Kontrolle der Systemkonfiguration: sind die Systeme entsprechend der Dokumentation konfiguriert.
- Kommunikationstest im Netzwerk: sind alle Systeme einwandfrei konfiguriert und angeschlossen.
- Loop Check: Kontrolle aller E/A-Signale im Diagnosemodus von GA safeEdit und in der Visualisierung. Alle Signale müssen von Kabelbruch über Minimum (analoge Erfassung der Digitalsignale) bis Maximum und Kurzschluss getestet werden. Die

Diagnose muss Fehlerzustände im Engineering- und Visualisierungssystem korrekt anzeigen.
- Funktionskontrolle aller Sicherheitsfunktionen im Stillstand der Maschine/Anlage.
- Funktionskontrolle aller Sicherheitsfunktionen bei laufender Maschine/Anlage.
- Datensicherung und Dokumentation aller durchgeführten Änderungen.
- Am Ende der Inbetriebnahme ist der sichere Normalbetrieb der Anlage herzustellen und zu Überprüfen: Betriebsart „Running“ eingestellt, keine Signale geforct, alle Zugriffe über Passwörter eingeschränkt.

7.3 Software-Programmänderungen

7.3.1 Programmänderungen und Erweiterungen

Vor Änderungen am Programm muss eine Einflussanalyse erfolgen:
- Alte Version ausdrucken, evtl. Datensicherung durchführen.
- Programmänderungen planen, neue Version erstellen mit GA safeEdit.
- Neue Version sichern und ausdrucken.
- Querverbindungen der geänderten Funktionsbausteine kontrollieren, im Grafikeditor.
- Betroffene Sicherheitsfunktionen, einschließlich Querverbindungen, analysieren: hat die neue Version nur die gewünschte Auswirkung und – auch bei den Querverbindungen – keine Nebenwirkungen?
  Bei Verbindung zu Betriebsartenumschaltungen den Umschaltzeitpunkt genau kontrollieren.
- Neue Version testen, mit Simulation und auf Zielhardware im Maschinenstillstand.
- Systemreaktionszeit mit neuer Version kontrollieren.
- Nach Abschluss der Änderungen die neue Version dokumentieren und Datensicherung anlegen.

7.3.2 Parametrierung ändern

Vor Änderungen an Programmparametern muss eine Einflussanalyse erfolgen:
- Datensicherung durchführen.
- Parameteränderungen planen.
- Querverbindungen der zu parametrierenden Funktionsbausteine kontrollieren, im Grafikeditor.
- Betroffene Sicherheitsfunktionen, einschließlich Querverbindungen, analysieren: hat die Änderung überall nur den gewünschten Effekt?
- Bei Skalierungsänderungen von E/A-Signalen auch die entsprechende Anpassung im Visualisierungssystem berücksichtigen.
- Neue Version testen.
- Nach Abschluss der Parametrierung die neue Version dokumentieren und Datensicherung durchführen.

7.3.3 Online-Änderung

Alle Programmänderungen sollen nach Möglichkeit bei stehender Maschine durchgeführt werden, da während der Änderungen die Sicherheitsintegrität des Systems eingeschränkt ist. Bei fehlerhafter Durchführung werden die Sicherheitsanforderungen nicht mehr erfüllt.

Grundsätzlich sind Änderungen bei laufender Maschine möglich. Dazu sind die folgenden Punkte zu beachten:

- Einflussanalyse wie bei normaler Programmänderung.
- Zusätzlich Einflussanalyse von Einschaltvorgängen.
- Berücksichtigung von unterschiedlichen Signalzuständen in den Einheiten des DUPLEX-S Systems während des Umprogrammierens der einzelnen Einheiten.
- Die Einheiten müssen getrennt programmiert werden. Nach Programmierung jeder Einheit muss hier der planungsgemäße Zustand aller E/A-Signale und internen Zustände kontrolliert werden. Eventuell ist ein Abgleich der Zustände durch Forcen von Signalen erforderlich.
- Während des gesamten Zeitraums sind angemessene externe Sicherungsmaßnahmen zu berücksichtigen, siehe auch Kapitel *Forcen von E/A-Signalen* auf Seite 28.
- Da Sicherheitsfunktionen während des Zeitraums betroffen sind müssen entsprechende Notfallmaßnahmen vorbereitet werden.

7.4 Inbetriebnahme, Checklisten

Nr.	Beschreibung	Check
1	Projektabhängiges Sicherheitskonzept eindeutig verstanden	
2	erforderliche Schlüsselschalter vorhanden, Passwörter bekannt	
3	System-Hardwarekonfiguration korrekt	
4	Kommunikationstest mit allen Systemen erfolgreich	
5	Loop-check für E/A Signale: Wertebereiche und Signal-Diagnosen	
6	Sicherungs- und Notfallmaßnahmen entsprechend vornehmen	
7	Sicherheitsfunktionen testen, im Stillstand, dann bei laufender Maschine	
7a	Bei Bedarf: Änderungen vornehmen, siehe Checkliste Programmänderung	
8	Systemreaktionszeiten kontrollieren	
9	Sicheren Betriebszustand herstellen	
10	Datensicherung	

Tabelle 7: Checkliste Inbetriebnahme

Nr.	Beschreibung	Check
1	Datensicherung	
2	Programmänderung im Stillstand oder Online	
3	Änderungsplanung mit Einflussanalyse entsprechend vornehmen, dabei die Liste der SIL3-geprüften Funktionsblöcke berücksichtigen	
4	Sicherungs- und Notfallmaßnahmen entsprechend vornehmen	
5	Implementierung und Test der neuen Softwareversion	
6	Systemreaktionszeiten kontrollieren	
7	Dokumentation der erfolgreichen Änderungen	
8	Datensicherung	

Tabelle 8: Checkliste Inbetriebnahme, Programmänderung

8 Wartung

8.1 Personelle Qualifikationen

Wartungsarbeiten müssen ausschließlich durch qualifiziertes Personal erfolgen. Dieses Personal muss mit den Warnungen und Hinweisen der technischen Handbücher vertraut sein.
Qualifiziertes Personal im Sinne der technischen Hardwarebeschreibungen sind Personen, die mit Aufstellung, Montage, Inbetriebnahme und Betrieb dieser Hardware vertraut sind und über die ihren Tätigkeiten entsprechenden Qualifikationen verfügen, wie z.B.:

- Ausbildung und Unterweisung bzw. Berechtigung, Stromkreise und Baugruppen bzw. Systeme gemäß den aktuellen Standards der Sicherheitstechnik ein- und auszuschalten, zu erden und zu kennzeichnen.
- Ausbildung und Unterweisung in der Verwendung der Software GA safeEdit zur Diagnose und Wartung.
- Einweisung in das projektspezifische Sicherheitskonzept.
- Ausbildung und Unterweisung gemäß den aktuellen Standards der Sicherheitstechnik in Pflege und Gebrauch angemessener Sicherheitsausrüstungen.
- Schulung in Erster Hilfe.

8.2 Vorgehensweise

Die Wartungsaufgaben teilen sich auf in reguläre Aufgaben und außerplanmäßige Aufgaben. Reguläre Aufgaben sind im Sicherheitskonzept konkret berücksichtigt und werden in den spezifizierten Wartungsintervallen anhand der Vorgaben durchgeführt. Dazu gehören z.B.:

- Proof-Test Intervalle
- Kontrolle oder Wechsel der Luftfilter
- Kontrolle auf Verschmutzung
- Kontrolle von Systemdiagnoseanzeigen wie: Diagnose-Visualisierung im DCS, Alarmierungen, LED Anzeigen der Hardwarekomponenten, erweiterte Diagnosen im Engineering-System mit GA safeEdit

Außerplanmäßige Aufgaben werden erforderlich wenn die regulären Kontrollen eine Systemstörung anzeigen. Sie sind im Sicherheitskonzept allgemein berücksichtigt. Es handelt sich z.B. um folgende Aufgaben:

- E/A-Signalfehler identifizieren und beheben
- Systemkomponenten-Fehler identifizieren, Komponenten (E/A-Karten, Lüfter, Netzteile, ...) ersetzen
- Netzwerkkommunikation kontrollieren und Fehler beheben

Bei außerplanmäßigen Wartungsaufgaben ist die folgende Vorgehensweise einzuhalten:

- Eindeutige Identifizierung von Fehlermeldungen und Fehlerursachen: z.B. kann eine zu hohe Systemtemperatur verschiedene Ursachen haben: Luftfilter verschmutzt, System-Lüfter defekt, Schaltschrank-Klimagerät defekt.
- Kontrolle des erkannten oder gemeldeten Fehlers mit den zur Verfügung stehenden Mitteln: Visualisierung im DCS, Kontrolle der Hardware (optisch, LEDs, ...), Kontrolle mit dem Engineering-System für erweiterte Diagnosezugriffe.
- Analyse der Fehlerauswirkung auf Sicherheit und Verfügbarkeit des Gesamtsystems.
- Planung der auszuführenden Wartungsaufgaben.
- Planung der erforderlichen Sicherheits- und Notfallmaßnahmen.

8.3 Komponenten-Austausch

Der Austausch von Systemkomponenten ist im laufenden Betrieb möglich, siehe *GA DUPLEX-S Racks technische Beschreibung*

Der Austausch der programmierbaren Systemkomponenten, MCxxx-S Karten und ICU-Karten, ist im laufenden Betrieb möglich und erfolgt nach folgender Vorgehensweise:

- Der Austausch erfordert den Einsatz des Engineering-Systems mit GA safeEdit.
- Das PES-System wird in den Maintenance-Modus geschaltet.
- Passwortgeschützte Verriegelungen werden mit dem entsprechenden Passwort aufgehoben.
- Der aufgetretene Fehler wird genau analysiert und dokumentiert.
- Die fehlerhafte Karte wird aus dem System entnommen.
- Hardware-Einstellmöglichkeiten (Jumper, Schalter, ...) der Reservekarte werden mit der fehlerhaften Karte verglichen und in Übereinstimmung gebracht.
- Die Reservekarte wird in das System gesteckt.
- Die Konfiguration der Reservekarte wird kontrolliert und bei Bedarf angepasst. Die korrekte Erkennung und Konfiguration der Karte wird in GA safeEdit angezeigt.
- Bei E/A-Karten:
  - Die Programmierung der Karte wird kontrolliert. Normalerweise muss das aktuelle Programm auf die Karte heruntergeladen werden.
  - Die Steckverbinder mit Feldsignalen werden aufgesteckt und verschraubt.
  - Der ordnungsgemäße Stand der Ein-/Ausgänge und interner Speicherzustände wird mit den redundanten Karten der anderen DUPLEX-Einheiten kontrolliert.
- Das System wird mit der neuen Karte getestet.
- Das System wird in den Running-Modus zurückgesetzt.

Weitere Details zum Austausch von Karten können der entsprechenden technischen Beschreibung der Karten entnommen werden. Weitere Hinweise zu Konfiguration und Programmierung stehen im *GA safeEdit Benutzerhandbuch*.

8.4 Wartung, Checkliste

Die Kontrolle der regulären Wartung, einschließlich Wiederholungsprüfung (Proof-Test), erfolgt anhand der projektspezifischen Wartungsvorgaben.

Nr.	Beschreibung	Check
1	Eindeutige Fehleridentifizierung: Stimmen Diagnosemeldungen aus Visualisierung, Engineering-System und LED-Zuständen der Karte miteinander überein?	
2	Ist die Vorgehensweise zum Kartenaustausch eindeutig verstanden?	
3	Sind die notwendigen Sicherheits- und Notfallmaßnahmen vorbereitet?	
4	Ist die neue Karte im System richtig konfiguriert und erkannt?	
5	Ist die neue Karte richtig programmiert?	
6	Stimmen interne und externe Signale mit den Karten der redundanten Systeme überein?	
7	Funktionieren die E/A-Signale richtig?	
8	Ist das System nach Beendigung der Wartungsarbeiten wieder im sicheren Zustand?	

Tabelle 9: Checkliste Wartung, Kartenaustausch

9 Zugangsberechtigung

9.1 Benutzeranmeldung

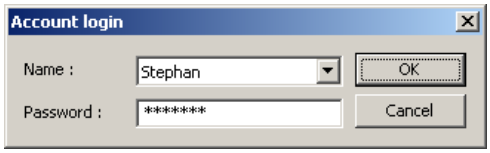

Abbildung 13: Benutzeranmeldung

Bevor man mit GA safeEdit arbeiten und so auf die GA DUPLEX-S Sicherheitssysteme zugreifen kann, muss man sich als berechtigter Benutzer anmelden. Dazu wählt man im Anmelde-Dialogfenster einen Benutzernamen aus der Liste und gibt das dazugehörige Passwort ein.
In der Liste gibt es immer den Namen „Admin“ sowie je nach Konfiguration einen oder mehrere Benutzer.

Ein angemeldeter Benutzer kann je nach seinen Berechtigungen mit dem System arbeiten. Änderungen an der Benutzerliste kann nur Admin vornehmen. Für Benutzer mit der höchsten Priorität sind Diagnosen, Konfigurations- und Programmänderungen der ICU Kommunikationsprozessoren und der E/A-Karten erlaubt.
Alle Eingriffe in die PES-Systeme erfordern zusätzlich den Maintenance-Modus mit dem Hardware-Schlüsselschalter. Im Running-Modus ist nur Systemdiagnose möglich.

Benutzerkonfiguration und Berechtigungen sind im *GA safeEdit Benutzerhandbuch* beschrieben.

9.2 Schlüsselschalter

Abbildung 14: Schlüsselschalter Running/Maintenance

Mit dem Schlüsselschalter kann das PES-System zwischen den beiden Betriebsarten „Running“ und „Maintenance“, also dem sichern Normalbetrieb und dem Wartungsbetrieb umgeschaltet werden.

Im Wartungsbetrieb sind sicherheitsrelevante Eingriffe in das System vom Engineering-System aus möglich. Dazu gehört das Forcen von E/A-Signalen, das Programmieren der MCxxx-S Controller-Karten und das Konfigurieren des Systems. Der Maintenance-Modus

kann unter entsprechenden Sicherheitsvorkehrungen bei laufender Maschine verwendet werden, der Normalbetrieb der Maschine oder Anlage ist damit jedoch nicht zulässig.

Die „Running“-Betriebsart ist der sichere Normalbetrieb der Maschine.
Nach erfolgreicher Inbetriebnahme oder Wartung werden alle Force-Befehle für E/A-Signale aufgehoben, dann wird der Schlüsselschalter auf die „Running“-Position gesetzt und der Schlüssel abgezogen. In dieser Position sind keine externen Eingriffe vom Engineering-System in das PES-System mehr möglich. Diagnoseinformationen und Kommunikation stehen natürlich weiterhin zur Verfügung und können im Engineering- oder Visualisierungssystem entsprechend den jeweiligen Möglichkeiten angezeigt werden.

Im Maintenance-Modus geforcte E/A-Signale werden durch „Running“-Umschaltung nicht automatisch zurückgesetzt. Es erscheint allerdings eine entsprechende Warnung.

10 Diagnose und Fehlerbehebung

10.1 Verfügbarkeit von Diagnosedaten

Selbstteststatistik

Ein autorisierter Anwender kann die Informationen der Selbstteststatistik einer jeden Karte auslesen. Diese Informationen werden in den karteninternen Flashspeichern während des Betriebs hinterlegt. Der Zugriff erfolgt über GA safeEdit, siehe Benutzerhandbuch.

Logbuch von Meldungen

Auf der Engineering Station werden alle Systemmeldungen (Warnings, Messages, …) wie in einem Logbuch hinterlegt. Die aktuellen Meldungen werden in einem Meldefenster angezeigt und die Historie wird in einer Log-Datei gespeichert. Zusätzlich werden alle Meldungen einer Einheit A, B oder C in der jeweiligen ICU im Flashspeicher hinterlegt und können jederzeit von der Engineering-Station gelesen werden. Zum Aufbau der Fehlernachrichten siehe Kapitel *Fehlernachrichten und deren Auswertung* auf Seite 37.

Visualisierungssystem

Über Kommunikation stehen dem Visualisierungssystem (DCS) automatisch umfangreiche Diagnoseinformationen zu allen E/A-Signalen zur Verfügung: Kabelbruch, Kurzschluss, Signal geforct, bei Digitaldaten auch geforcter Zustand.
Zu allen E/A-Karten kann eine Lebensbit-Überwachung programmiert werden.
Zusätzlich stehen automatisch Systemtemperaturen und Systemspannungen der ICU-Kommunikationskarten zur Verfügung.

Die Aufzeichnung dieser Daten erfolgt entsprechend den Möglichkeiten des Visualisierungssystems.

10.2 Verfügbarkeit von Prozessdaten

Alle Prozessdaten stehen über eine Kommunikationsschnittstelle der Visualisierungseinheit (DCS, HMI-Workstation, …) online zur Verfügung. Die Datenaufzeichnung kann entsprechend den Möglichkeiten dieses Systems erfolgen.

Auf dem Engineering-System können mit der integrierten Trend-Analyse beliebige Prozessdaten online als Zeitdiagramm angezeigt und analysiert werden.

Echtzeit Datalogging aller E/A-Signale auf dem intelligenten Buscontroller (ICU) und Zeitsynchronisierung ist als Standard im Grundsystem möglich.

10.3 Fehlernachrichten und deren Auswertung

Im Engineering-System GA safeEdit stehen detaillierte Diagnoseinformationen zur Verfügung. Sobald ein nicht normales Systemverhalten auftritt werden entsprechende Fehlernachrichten angezeigt und im Logbuch aufgezeichnet.

Der Aufbau einer Fehlernachricht lässt sich anhand eines typischen Beispiels verdeutlichen:
`Fr, 16 Sep 2005 15:57:52 : MCU-S 192.168.100.183 (1): (1,13,0) Card Timeout (ID:116): unit:0, slot:6, timestamp:0xe377, time:0xe44f`

Zuerst werden Datum und Uhrzeit angegeben, wann die Fehlermeldung aufgetreten ist. In diesem Fall trat der Fehler am Freitag, den 16. Sep. 2005 um 15:57 auf.

Danach werden der Typ der versendenden CPU, die IP Adresse der ICU, die die Fehlermeldung der MCU-S weitergeleitet hat, und die Netzwerknummer angezeigt. MCU-S bedeutet, dass die Nachricht von einer Sicherheitskarte verschickt worden ist. In diesem Fall erfolgte die Fehlermeldung über die ICU mit der IP Adresse 192.168.100.183. Im Beispiel kommt die Meldung über das Netzwerk 1. (In DUPLEX-S Systemen können die einzelnen Units in unterschiedlichen Netzwerken liegen.)

Danach folgt die Position der MCU-S im System. Die Position wird in der Reihenfolge Unit (0: Unit A, 1: Unit B, *2: Unit C (nur in GA TMR-S)*), Slot (1-16) und MCU (0: MCU-A, 1: MCU-B) angezeigt. Für das Beispiel gilt: (1,13,0) bedeutet entsprechend der Beschreibung Unit B, Slot 13, MCU-A.

Abschließend folgt ein erläuternder Text zur Fehlermeldung, in diesem Fall „`Card Timeout (ID:116)` “. Im Text ist die Fehlernummer „ID:116“ angegeben. Anhand der Fehlernummer und der Fehlermeldung kann man in der *technischen Beschreibung* der Sicherheitskarte eine nähere Beschreibung der Fehlerursache sehen und erfahren wie man den Fehler beheben kann. Die Fehlernummer 116 führt in dem Fall zu den Erläuterungen zum Card Timeout.

Als zusätzliche Hilfe zur Fehleranalyse wird in der Fehlermeldung der Zeitpunkt, an dem das letzte Prozessdatenpaket der vom Card Timeout betroffenen Karte eingetroffen ist, und der aktuelle Zeitstempel angegeben.

11 Allgemeine Technische Daten

Elektrische Parameter Einspeisung	
nominale Betriebsspannung	100 ... 240 VAC, 50 ... 60 Hz
maximale Betriebsspannung	85 ... 264 VAC, 47 ... 63 Hz
Max. Power DUPLEX/7-S	450 W
Max. Power DUPLEX-SMART-S	300 W
Digitale – Eingänge MCDIN-S	
Eingangsstrom	nach Namur
“High level”-Strom	> 2,1 mA
“Low level”-Strom	< 1,2 mA
Analoge Eingänge MCAD-S	
Eingangsstrombereich	0 ... 25mA
Frequenzeingänge	100Hz ...15kHz
Digitale – Ausgänge MCDOT-S / DFAB	
Ausgangsspannung	24 VDC, 230VAC
Ausgangsstrom pro Kanal (max.)	0 ... 6A

Umweltanforderungen aller elektrischen Komponenten	
Umgebungstemperatur (Lagerung)	-25°C ... +70 °C
Umgebungstemperatur (Betrieb)	+0°C ... +55°C
Luftfeuchtigkeit	10% ... 90% nicht kondensierend
Schutzklasse nach IEC525	IP 20
Einsatzhöhe	bis 2000m
Verschmutzungsgrad	2
Schutzklasse für Netzanschluss	Schutzklasse I mit Schutzleiter
Schutzklasse für Feldanschlüsse	Schutzklasse III
Mechanische Daten Baugruppenträger	
DUPLEX/7-S (10HE / 84 TE)	482,6 x 324 x 391 mm [B x H x T]
DUPLEX SMART-S (4HE / 84 TE)	482,6 x 191 x 391 mm [B x H x T]

Weitere technische Daten und Informationen sind den jeweiligen *technischen Beschreibungen* zu entnehmen.

12 Sicherheitstechnische Angaben

12.1 Berechnungsgrundlage

In Systemen mit 1-aus-2D Auswahl berechnen sich die Versagenswahrscheinlichkeiten PFD und PFH folgendermaßen:

$$PFD_G = 2(1-\beta)\lambda_{DU} \cdot ((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD})t'_{CE}t'_{GE} + \beta_D\lambda_{DD} \cdot MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right)$$

$$PFH_G = 2 \cdot (1-\beta) \cdot \lambda_{DU} \cdot ((1-\beta) \cdot \lambda_{DU} + (1-\beta_D) \cdot \lambda_{DD} + \lambda_{SD}) \cdot t'_{CE} + \beta_D \cdot \lambda_{DD} + \beta \cdot \lambda_{DU}$$

mit:

$$t'_{CE} = \frac{\lambda_{DU} \cdot \left(\frac{T_1}{2} + MTTR\right) + (\lambda_{DD} + \lambda_{SD}) \cdot MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}}$$

$$t'_{GE} = \frac{\lambda_{DU} \cdot \left(\frac{T_1}{3} + MTTR\right) + (\lambda_{DD} + \lambda_{SD}) \cdot MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}}$$

$$\lambda_{SD} = \frac{\lambda}{2} \cdot DC$$

Der Anteil ungefährlicher Ausfälle (SFF, Safe Failure Fraction) berechnet sich als:

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_{DD} + \lambda_{DU}}$$

Der Diagnosedeckungsgrad (DC, Diagnostic Coverage) berechnet sich als:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_D} = \frac{\sum \lambda_{DD}}{\sum \lambda_{DD} + \sum \lambda_{DU}}$$

In den Formeln verwendete Faktoren:

Abkürzung	Beschreibung
β	Anteil unerkannter Ausfälle infolge gemeinsamer Ursache.
β_D	Anteil der Ausfälle infolge gemeinsamer Ursache, die durch Diagnosetest erkannt werden.
λ	Ausfallrate eines Kanals in einem Teilsystem (je Stunde)
λ_D	Rate gefahrbringender Ausfälle (je Stunde) eines Kanals eines Teilsystems (D = dangerous)
λ_{DD}	Rate erkannter gefahrbringender Ausfälle (je Stunde) eines Kanals eines Teilsystems (DD = dangerous, detected)
λ_{DU}	Rate unerkannter gefahrbringender Ausfälle (je Stunde) eines Kanals eines Teilsystems (DU = dangerous, undetected)
λ_S	Rate sicherer, nicht gefahrbringender Ausfälle (je Stunde) eines Kanals eines Teilsystems (S = safe)
T_1	Intervall der Wiederholungsprüfung (in Stunden)

MTTR	Mittlere Zeit zur Wiederherstellung (Mean Time To Repair) (in Stunden)
DC	Diagnosedeckungsgrad
SFF	Anteil ungefährlicher Ausfälle (Safe Failure Fration)
PFD_G	Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung einer Gruppe von Kanälen mit Ausgangsvergleicher oder Mehrheitsentscheider (PFD = Probability of Failure on Demand)
PFH_G	Ausfallwahrscheinlichkeit je Stunde für eine Gruppe von Kanälen mit Ausgangsvergleicher oder Mehrheitsentscheider (PFH = Probability of Failure per Hour)
t_{CE}'	mittlere Äquivalenzunklarzeit (in Stunden), gemeinsame Unklarzeit für alle Komponenten in einem Kanal des Teilsystems
t_{GE}'	mittlere Äquivalenzunklarzeit (in Stunden) für eine Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider, gemeinsame Unklarzeit für alle Kanäle in einer Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider

12.2 Beispielrechnung

Als konkretes Berechnungsbeispiel wird ein redundantes System mit analoger Eingangskarte MCAD-S, digitaler Eingangskarte MCDIN-S, digitaler Ausgangskarte MCDOT-S und einem Ausgangs-Voter DFAB-1oo2D angenommen.

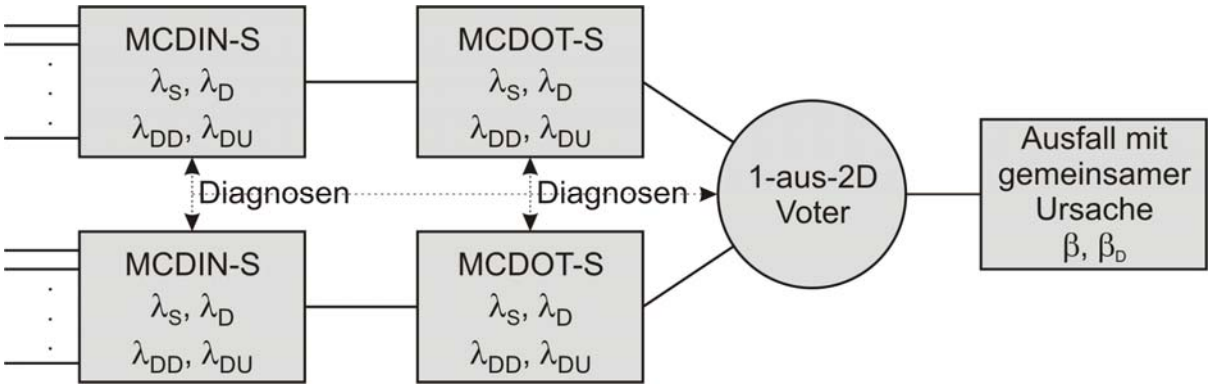

Abbildung 15: Zuverlässigkeits-Blockdiagramm für 1-aus-2D

Bei dieser Konfiguration hat man ein 1-out-of-2D System mit 2x 24 digitalen und 2x 24 analogen Eingangssignalen, die für Sicherheitsfunktionen miteinander verknüpft werden können. Mit den berechneten Zuständen können maximal 8 digitale Ausgangssignale angesteuert werden.

Für dieses System ergeben sich die folgenden Werte:

$T_1 = 8{,}7600 \cdot 10^{+3}$	(1 Jahr)	$T_1 = 8{,}7600 \cdot 10^{+4}$	(10 Jahre)
$MTTR = 8{,}0$		$MTTR = 8{,}0$	
$\beta = 2{,}0000 \cdot 10^{-2}$		$\beta = 2{,}0000 \cdot 10^{-2}$	
$\beta_D = 1{,}0000 \cdot 10^{-2}$		$\beta_D = 1{,}0000 \cdot 10^{-2}$	
$\lambda_S = 8{,}9106 \cdot 10^{-5}$		$\lambda_S = 8{,}9106 \cdot 10^{-5}$	
$\lambda_D = 1{,}2444 \cdot 10^{-6}$		$\lambda_D = 1{,}2444 \cdot 10^{-6}$	
$\lambda_{DD} = 1{,}2343 \cdot 10^{-6}$		$\lambda_{DD} = 1{,}2343 \cdot 10^{-6}$	
$\lambda_{DU} = 1{,}0095 \cdot 10^{-8}$		$\lambda_{DU} = 1{,}0095 \cdot 10^{-8}$	
$t'_{CE} = 8{,}9601$		$t'_{CE} = 1{,}7601 \cdot 10^{+1}$	
$t'_{GE} = 8{,}6401$		$t'_{GE} = 1{,}4401 \cdot 10^{+1}$	
$\boldsymbol{PFD_G = 9{,}8469 \cdot 10^{-7}}$		$\boldsymbol{PFD_G = 8{,}9436 \cdot 10^{-6}}$	
$\boldsymbol{PFH_G = 1{,}2553 \cdot 10^{-8}}$		$\boldsymbol{PFH_G = 1{,}2561 \cdot 10^{-8}}$	
$\boldsymbol{SFF = 99{,}9888\%}$		$\boldsymbol{SFF = 99{,}9888\%}$	
$\boldsymbol{DC = 99{,}19\%}$		$\boldsymbol{DC = 99{,}19\%}$	

Bei einer erfahrungsgemäß realistischen Aufteilung der Ausfallwahrscheinlichkeiten von 15% für das PES-System, 35% für Sensor + Transmitter und 50% für Aktor ergibt sich enstprechend der IEC 61508 Tabelle zur Ausfallwahrscheinlichkeit die Einstufung für das GA DUPLEX-S System inklusive Sensoren und Aktoren:

SIL 15%	PFD	PFH
1	$\geq 1{,}5 \cdot 10^{-3}$ bis $< 1{,}5 \cdot 10^{-2}$	$\geq 1{,}5 \cdot 10^{-7}$ bis $< 1{,}5 \cdot 10^{-6}$
2	$\geq 1{,}5 \cdot 10^{-4}$ bis $< 1{,}5 \cdot 10^{-3}$	$\geq 1{,}5 \cdot 10^{-8}$ bis $< 1{,}5 \cdot 10^{-7}$
3	$\geq 1{,}5 \cdot 10^{-5}$ bis $< 1{,}5 \cdot 10^{-4}$	$\geq 1{,}5 \cdot 10^{-9}$ bis $< 1{,}5 \cdot 10^{-8}$
4	$\geq 1{,}5 \cdot 10^{-6}$ bis $< 1{,}5 \cdot 10^{-5}$	$\geq 1{,}5 \cdot 10^{-10}$ bis $< 1{,}5 \cdot 10^{-9}$

Tabelle 10: 15% PES-Ausfallwahrscheinlichkeiten und SIL-Einstufung

Enstprechend der IEC 61508 Tabelle zur Sicherheitsintegrität der Hardware, Typ B-Teilsysteme, ergibt sich für das GA DUPLEX-S System:

SFF	Fehlertoleranz der Hardware (HFT)		
	0	1	2
< 60 %	nicht erlaubt	SIL 1	SIL 2
60 % bis < 90 %	SIL 1	SIL 2	SIL 3
90 % bis < 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Tabelle 11: Sicherheitsintegrität der Hardware, Typ B-Teilsysteme

Die für die Einstufung in SIL 3 nach IEC 61508 erforderlichen Grenzwerte werden unter Berücksichtigung der 15% Aufteilung für das PES in diesem Anwendungsbeispiel also sehr gut eingehalten bzw. deutlich übertroffen.

13 Index

Berechnungen
- Ausfallrate **39**
- Ausfallwahrscheinlichkeit **40**
- DC **40**
- Fehlertoleranz **41**
- HFT **41**
- MTTR **40**
- PFD **39**, **41**
- PFH **39**, **41**
- SFF **40**, **41**
- Wiederholungsprüfung **21**, **39**

BITs **14**
DCS **12**, 13, 23, 25, 29, 32, 36
Diagnose Testintervall **20**
Engineering 22
- Hardware **22**
- Software **23**
- System **12**, 29, 32, 33, 34, 35, 36

Fehlernachricht **37**
Fehlerreaktion 14, **20**
GA DUPLEX-S 9, 12, 13, 19, 20, 34
GA safeEdit 12, 23, 24, 26, 29, 30, 32, 33, 34, 36, 37
IEC 61508 ..... 7, **10**, **41**
Karten
- DSPVCU **18**
- FPR **17**
- ICU 13, **17**, 33, 34, 36, 37
- MCAD-S 13, 38
- MCDIN-S 13, 16, 38
- *MCDOT-S* 20, 22, 23, 24, 25, 38
- MCxxx-S **16**, 17, 33, 34

Kommunikation 12, 17, 30, 35, 36
Lebenszyklus 10
Maintenance 25, 29, 33, 34, 35
PES-System **12**, 20, 21, 22, 23, 24, 25, 28, 33
Prozessdaten **36**, 37
Running 30, 33, 34, 35
Schlüsselschalter 12, 29, 31, **34**
Selbsttest **14**, 20, 36
Sicherheitslebenszyklus **10**
Sicherheitszeit 20, **21**, 23, 24, 25
SIL3 geprüfte Funktionen 24, 25, 31
Systemreaktionszeit **20**, 21, 22, 23, 24, 25, 30, 31
Trend-Analyse **36**
Visualisierungssystem **12**, 23, 24, 30, 35, 36
Wiederholungsprüfung **21**
Zeitsynchronisierung **36**
Zertifikat **7**